# Table of Contents

1 **Introduction** ........................................................................................................................................ 1
   1.1 Organization of This Guidebook .................................................................................................... 1
   1.2 Audience ........................................................................................................................................ 2
   1.3 Applicability ................................................................................................................................... 2
   1.4 Terminology ................................................................................................................................... 2

2 **Cybersecurity Policies and Guidance for Defense Acquisition Programs and Systems** .............. 3
   2.1 Operation of the Defense Acquisition System, DoDI 5000.02 ...................................................... 3
   2.2 Business Systems Requirements and Acquisition, DoDI 5000.75 ................................................. 3
   2.3 Cybersecurity, DoDI 8500.01 ........................................................................................................ 4
   2.4 Joint Requirements Guidance ......................................................................................................... 6
   2.5 DOT&E Cybersecurity Procedures Memoranda ............................................................................ 6

3 **Cybersecurity Test and Evaluation Overview** ................................................................................. 7
   3.1 Cybersecurity T&E Phases Overview ............................................................................................ 7
   3.2 Cybersecurity Working Group ....................................................................................................... 9
   3.3 Cybersecurity Threat Assessments ............................................................................................... 10
   3.4 DT&E and SE Collaboration ......................................................................................................... 10
   3.5 Early Tester/Analyst Involvement ................................................................................................ 12
   3.6 Mission-Based Cyber Risk Assessments ..................................................................................... 12
   3.7 Role of Cybersecurity Developmental Testing ............................................................................ 12
   3.8 DT&E and OT&E Collaboration .................................................................................................  15

4 **Phase 1: Understand Cybersecurity Requirements (and Plan for T&E)** .................................... 17
   4.1 Schedule ....................................................................................................................................... 17
   4.2 Inputs ............................................................................................................................................ 18
   4.3 Tasks ............................................................................................................................................ 18
   4.4 Outputs ......................................................................................................................................... 21

5 **Phase 2: Characterize the Cyber-Attack Surface** ........................................................................... 23
   5.1 Schedule ....................................................................................................................................... 23
   5.2 Inputs ............................................................................................................................................ 24
   5.3 Tasks ............................................................................................................................................ 25
   5.4 Outputs ......................................................................................................................................... 32

6 **Phase 3: Cooperative Vulnerability Identification** ......................................................................... 35
   6.1 Schedule ....................................................................................................................................... 36
   6.2 Inputs ............................................................................................................................................ 36
   6.3 Tasks ............................................................................................................................................ 37
6.4 Outputs ......................................................................................................................................... 43

7 Phase 4: Adversarial Cybersecurity DT&E ................................................................................... 45
   7.1 Schedule .................................................................................................................................. 45
   7.2 Inputs ................................................................................................................................ ...... 46
   7.3 Tasks ...................................................................................................................................... 46
   7.4 Outputs .................................................................................................................................. 50

8 Phase 5: Cooperative Vulnerability and Penetration Assessment ............................................... 51
   8.1 Schedule ................................................................................................................................ 51
   8.2 Inputs ...................................................................................................................................... 52
   8.3 Tasks ...................................................................................................................................... 52
   8.4 Outputs .................................................................................................................................. 54

9 Phase 6: Adversarial Assessment .................................................................................................... 55
   9.1 Schedule ................................................................................................................................ 55
   9.2 Inputs ...................................................................................................................................... 55
   9.3 Tasks ...................................................................................................................................... 56
   9.4 Outputs .................................................................................................................................. 57

10 Acronyms and Glossary of Terms ................................................................................................. 58
   10.1 Acronyms ........................................................................................................................... 58
   10.2 Cybersecurity T&E Glossary of Terms ............................................................................... 61

11 References ..................................................................................................................................... 67

Appendix A Cybersecurity T&E Phase 1 through 6 Quick Look .................................................. A-1
Appendix B Incorporating Cybersecurity T&E into DoD Acquisition Contracts ...................... B-1
Appendix C Considerations for Tailoring the Cybersecurity T&E Phases ................................. C-1
Appendix D Key System Artifacts for Cybersecurity T&E Analysis and Planning .................. D-1
Appendix E Guidance for the Cybersecurity Portion of the DEF ............................................. E-1
Appendix F Considerations for Staffing Cybersecurity T&E Activities ..................................... F-1
Appendix G Considerations for Software Assurance Testing ..................................................... G-1
Appendix X1 Considerations for Cybersecurity Requirements and Measures for DT&E (FOUO Document) .......................................................... X-1
Appendix X2 Appendix X2 Cyber Threat Assessment for Cybersecurity T&E (FOUO Document) ........................................................................ X-1
Appendix X3 Mission-Based Cybersecurity Risk Assessments (FOUO Document) ............... X-1
Appendix X4 Cybersecurity Test Infrastructure and Environment Planning (FOUO Document) X-1
Appendix X5 Cybersecurity Test Considerations for Non-IP Systems (FOUO Document) ........ X-1
List of Figures

Figure 2-1. Business Capability Acquisition Cycle ........................................................................... 4
Figure 2-2. RMF Icon .......................................................................................................................... 5
Figure 3-1. Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle ........................................ 7
Figure 3-2. Cybersecurity T&E Phases Are Iterative .......................................................................... 9
Figure 3-3. Interaction of SE and T&E Cybersecurity Activities .......................................................... 11
Figure 3-4. Interaction of RMF and T&E Cybersecurity Activities ......................................................... 14
Figure 4-1. Phase 1: Understand Cybersecurity Requirements Activities .............................................. 17
Figure 4-2. Phase 1 Iteration ................................................................................................................ 18
Figure 5-1. Phase 2: Characterize the Cyber-Attack Surface Activities ................................................ 23
Figure 5-2. Phase 2 Iteration ................................................................................................................ 24
Figure 5-3. Example Mission Decomposition and Criticality Analysis .................................................. 27
Figure 5-4. Example Cyber-Attack Surface System Diagram ............................................................... 28
Figure 5-5. Cyber Kill Chain ............................................................................................................... 30
Figure 5-6 Example Attack Surface Analysis ....................................................................................... 31
Figure 6-1. Phase 3: Cooperative Vulnerability Identification Activities ................................................ 35
Figure 6-2. Phase 3 Testing Process ..................................................................................................... 36
Figure 6-3. Phase 3 Iteration ................................................................................................................ 36
Figure 7-1. Phase 4: Adversarial Cybersecurity DT&E Activities .......................................................... 45
Figure 8-1. Phase 5: Cooperative Vulnerability and Penetration Assessment Activities ....................... 51
Figure 9-1. Phase 6: Adversarial Assessment Activities Schedule ....................................................... 55
Figure C-1. Waterfall Release Cycle .................................................................................................. C-5
Figure C-2. Agile Release Cycle ......................................................................................................... C-6
Figure C-3. Notional Division of Security Inheritance and Risk ............................................................ C-9
Figure C-4. Cybersecurity T&E Phases Mapped to the BCAC Process ................................................ C-10
Figure E-1. DEF Schedule .................................................................................................................. E-1
Figure E-2. Developmental Evaluation Framework Format .................................................................. E-3
Figure E-3. Example DEF Completed Cybersecurity Section ............................................................... E-6
Figure F-1. Example RASCI Table ...................................................................................................... F-7
Figure G-1. Software Stack Example .................................................................................................. G-2
Figure G-2. Compromising the Software Stack ..................................................................................... G-2
Figure G-3. Windows Architecture ..................................................................................................... G-4
Figure G-4. Software Testing Strategy ................................................................................................ G-5
Figure G-5. Software Testing Schedule ............................................................................................... G-7
Figure G-6. Testing Rigor ....................................................................................................................... G-11
Figure G-7. Comprehensive Evaluation of System Reliability ............................................................... G-13
List of Tables

Table 4-1. Cybersecurity and Resilience Requirements and Testing Factors to Consider ........................................... 19
Table 5-1. Mobile Navigation System (Notional) Attack Surface List ................................................................. 25
Table 6-1. Example Evaluation Goals, Test Objectives and Metrics ................................................................. 38
Table 6-2. Example Test Activities .................................................................................................................... 40
Table 6-3. Cybersecurity DT&E Activities and Cybersecurity Test Facilities .................................................. 41
Table A-1. Cybersecurity T&E Acquisition and Review Decisions Quick Look .............................................. A-1
Table A-2. Quick-Look Summary of DT&E Cybersecurity Phases 1 through 4 ................................................. A-2
Table A-3. Quick-Look Summary of OT&E Cybersecurity Phases 5 and 6 ......................................................... A-4
Table A-4. Phase 1 – Understand Cybersecurity Requirements and Plan for T&E Quick Look ..................... A-5
Table A-5. Phase 2 – Characterize the Cyber Attack Surface Quick Look ...................................................... A-6
Table A-6. Phase 3 – Cooperative Vulnerability Identification Quick Look .................................................. A-7
Table A-7. Phase 4 – Adversarial Cybersecurity DT&E Quick Look ............................................................. A-8
Table A-8. Phase 5 – Cooperative Vulnerability and Penetration Assessment Quick Look ............................. A-9
Table A-9. Phase 6 – Adversarial Assessment Quick Look ................................................................................ A-9
Table C-1. Compressed Cybersecurity Analysis Risks ....................................................................................... C-3
Table C-2. Integrated Cybersecurity DT&E/OT&E .......................................................................................... C-4
Table C-3. BCAC Acquisition Decisions Informed by Cybersecurity T&E .................................................... C-10
Table G-1. Cybersecurity Software Test Requirements .................................................................................. G-7
Table G-2. Characterization Sources ............................................................................................................... G-8
Table G-3. Sample Test Methods .................................................................................................................... G-9
1 Introduction

The purpose of this updated guidebook is to promote data-driven mission-impact-based analysis and assessment methods for cybersecurity test and evaluation (T&E) and to support assessment of cybersecurity, survivability, and resilience within a mission context by encouraging planning for tighter integration with traditional system T&E. Cybersecurity T&E starts at acquisition initiation and continues throughout the entire life cycle.

The guidebook supplements information provided in the Test and Evaluation Master Plan (TEMP) Guidebook. For more information about TEMPs see References. This updated version avoids restating policy, such as that in the Risk Management Framework (RMF); instead, it encourages the reader to go directly to policy source documents for more information.

1.1 Organization of This Guidebook

This guidebook has nine chapters, including this introductory Chapter 1. Chapter 2 describes the policies and guidance that are the basis for cybersecurity T&E activities described in this guidebook. Chapter 3 provides an overview of cybersecurity T&E. Chapters 4 through 9 provide detailed implementation guidance for PMs and test organizations on each of the phases of cybersecurity T&E as follows:

- Chapter 4: Phase 1—Understand Cybersecurity Requirements
- Chapter 5: Phase 2—Characterize the Cyber-Attack Surface
- Chapter 6: Phase 3—Cooperative Vulnerability Identification
- Chapter 7: Phase 4—Adversarial Cybersecurity DT&E
- Chapter 8: Phase 5—Cooperative Vulnerability and Penetration Assessment
- Chapter 9: Phase 6—Adversarial Assessment

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

- Appendix A: Cybersecurity T&E Phase 1 through 6 Quick Look
- Appendix B: Incorporating Cybersecurity T&E into DoD Acquisition Contracts
- Appendix C: Considerations for Tailoring the Cybersecurity T&E Phases
- Appendix D: Key System Artifacts for Cybersecurity T&E Analysis and Planning
- Appendix E: Guidance for the Cybersecurity Portion of the Developmental Evaluation Framework (DEF)
- Appendix F: Considerations for Staffing Cybersecurity T&E Activities
- Appendix G: Considerations for Software Assurance Testing
- Appendix X1: Considerations for Cybersecurity Requirements and Measures for Developmental T&E (FOUO document)
- Appendix X2: Cyber Threat Assessment for Cybersecurity T&E (FOUO document)
- Appendix X3: Mission-Based Cybersecurity Risk Assessment (FOUO document)
- Appendix X4: Cybersecurity Test Infrastructure and Environment Planning (FOUO document)
- Appendix X5: Cybersecurity Test Considerations for Non-IP Systems (FOUO document)

For Official Use Only (FOUO) appendices are accessible to government and authorized contractor personnel at the following link:
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx
1.2 Audience

This guidebook is intended for PMs, Chief Developmental Testers (CDTs), Lead DT&E Organizations, Operational Test Agencies (OTAs), and the cybersecurity test teams for Department of Defense (DoD) acquisition programs.

1.3 Applicability

The guidance applies to all DoD acquisition programs and systems (e.g., defense business systems (DBS), national security systems, weapon systems, non-developmental items) regardless of their acquisition category (i.e., ACAT I, IA, II III, IV) or their phase of the acquisition life cycle unless noted. Acquisition programs not required to follow DoDI 5000 series guidance will also benefit from following this guidebook.

1.4 Terminology

Cybersecurity T&E or the abbreviation CSTE is used to describe the activities that encompass all cybersecurity test and evaluation activities, including vulnerability assessments, security controls testing, penetration testing, adversarial testing, and cybersecurity testing related to a system’s resiliency and survivability capabilities.

The Services/Components and organizations involved in cybersecurity T&E may use different terms for the people or teams discussed in the guidebook. The activities described in this document are more important than the titles of those performing the activities. For example, the term “cybersecurity tester,” as used often in this guidebook, refers to individual analysts and vulnerability or adversarial assessment teams, including Blue and Red Teams, involved in the verification and validation of system cybersecurity capabilities, requirements, and resiliency across the life cycle of a system. Appendix F generally addresses key personnel involved in the testing planning, analysis, and execution.

The Services/Components may also use different terms for their assessments of system cyber resiliency. This guidebook uses the phrase Prevent, Mitigate, Recover (PMR) for consistency with the key attributes described in the Cyber Survivability Endorsement Implementation Guide (CSEIG)v1.01. PMR is defined as:

- **Prevent**: The ability to protect critical mission functions from cyber threats.
- **Mitigate**: The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.
- **Recover**: The resilience to recover from cyber-attacks and prepare mission systems for the next fight.

Further discussion of the CSEIG is found in this guidebook in Section 2.4 and Appendix X1.
2 Cybersecurity Policies and Guidance for Defense Acquisition Programs and Systems

This chapter summarizes policy for planning and conducting cybersecurity T&E.

2.1 Operation of the Defense Acquisition System, DoDI 5000.02

DoD Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, updated in 2017 with Enclosure 14, Cybersecurity in the Defense Acquisition System, outlines responsibilities the PM must implement to safeguard DoD acquisition systems from cybersecurity-related risks throughout the system life cycle.

The key T&E elements of the policy are its emphasis on the continuous need to understand adverse mission impacts from cyber-attacks by using evolving system threats to inform operational impacts. “Paragraph 3.b. (4) explains the goal is to mitigate risks that could impact performance objectives as well as thresholds.” This updated guidebook integrates this increased emphasis on understanding threats and mission-based cybersecurity risks.

This guidebook outlines the preferred approach for PMs, CDTs, and OTAs to implement the DoDI 8500.01 and DoDI 5000.02 policies for cybersecurity T&E.

2.2 Business Systems Requirements and Acquisition, DoDI 5000.75

DoDI 5000.75, Business Systems Requirements and Acquisition, first published in February 2017, defines policy and procedures, including cybersecurity for DBS. It outlines responsibilities the PM must implement to safeguard DoD business systems throughout the system life cycle.

The policy describes the use of the Business Capability Acquisition Cycle (BCAC) for business systems requirements and acquisition. DoDI 5000.75 supersedes DoDI 5000.02 for all business system acquisition programs that are not designated as a Major Defense Acquisition Program (MDAP) (based on MDAP thresholds) according to DoDI 5000.02. The notable difference between the BCAC and the traditional acquisition life cycle are that the BCAC has different phase names and six milestone decisions (depicted in Figure 2-1) instead of three.

---

1 DoDI 5000.02, Operation of the Defense Acquisition System, Enclosure 14 (7 January 2017)
The policy states that the Program Office’s implementation plan must include cybersecurity processes to reduce technical risk through T&E management procedures that include:

- A DEF
- Cooperative vulnerability identification and adversarial cybersecurity testing in both developmental and operational tests
- A Cyber Economic Vulnerability Analysis (CEVA) as outlined in the January 21, 2015, Director, Operational Test and Evaluation (DOT&E) Memoranda—CEVA is required at the discretion of DOT&E only for DoD systems whose functions include financial or fiscal/business activities or the management of funds
- Direction to Milestone Decision Authorities (MDAs) to avoid tailoring cybersecurity T&E solely to meet Authorization to Operate (ATO) requirements

Appendix C includes considerations for tailoring the cybersecurity T&E phases for the BCAC.

### 2.3 Cybersecurity, DoDI 8500.01

DoDI 8500.01, *Cybersecurity*, defines the policy and procedures for cybersecurity. The key elements of the policy are that it:

- Extends applicability to all DoD information technology (IT), including Platform IT.
- Emphasizes operational resilience, integration, and interoperability.
- Incorporates cybersecurity considerations early and continuously within the acquisition life cycle.
- References the National Institute of Standards and Technology (NIST) Special Publication 800-53 Security Control Catalog for use in the DoD.

The policy defines the following activities for the CDT, Lead DT&E Organizations, and the T&E community:

- Ensure that cybersecurity T&E is conducted throughout the acquisition life cycle.
- Plan, resource, and integrate cybersecurity assessments into DT&E and as part of T&E assessments.
• Incorporate cybersecurity planning, implementation, testing, and evaluation in the DoD acquisition process and reflect these in the system TEMP.
• Ensure that cybersecurity T&E is integrated with interoperability and other functional testing, and that a cybersecurity representative participates in planning, execution, and reporting of integrated T&E activities.

Enclosure 3 states that acquisition programs must conduct an operational resilience evaluation during cybersecurity DT&E and operational T&E (OT&E). The evaluation includes exercising under realistic cyber conditions the ability to prevent and mitigate penetrations and exploitations and to recover data and information. To inform acquisition and fielding decisions, PMs must test procedures and tactics for workarounds and fallbacks in hostile environments. PMs must:

• Conduct periodic exercises or evaluations of a program’s ability to operate during loss of all information resources and connectivity.
• Ensure systems can allocate information resources dynamically as needed to sustain mission operations while addressing cybersecurity failures, no matter the cause.
• Ensure systems can restore information resources rapidly to a trusted state while maintaining support to ongoing missions.

Enclosure 3 also instructs PMs to include an evaluation of cybersecurity during an acquisition T&E event. The evaluation must include independent, threat representative penetration and exploitation T&E of the complete system cyberspace defenses, including the controls and protection that Cybersecurity Service Providers (CSSPs) deliver. PMs must plan and resource the penetration and exploitation testing part of DT&E and OT&E using the appropriate system test documentation.

DoDI 5000.02, Enclosure 14, DoDI 5000.75, and this guidebook contain the policy and guidance to ensure PMs successfully perform the above defined DoDI 8500.01 activities.

2.3.1 Risk Management Framework, DoDI 8510.01

The RMF, defined in NIST Special Publication 800-37, is mandated for the DoD by DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT). The policy defines procedures for acquisition processes for developmental T&E, but do not replace DT&E or OT&E. DoDI 8510.01 requires that the test community:

• Integrate RMF activities with developmental and operational test activities.
• Define specific concepts and rules for testing to support reciprocity between Program Offices to reduce redundant testing, assessments, documentation, and the associated costs in time and resources.

Integration of RMF with DT&E and OT&E processes requires proper and early planning to ensure that data needed for DT&E and OT&E is available. Look for the RMF icon, Figure 2-2, throughout this guidebook as an indicator to highlight RMF and T&E integration:

Figure 2-2. RMF Icon
2.4 Joint Requirements Guidance

In January 2017, the Joint Requirements Oversight Council (JROC) approved a proposed update to the Joint Capabilities Integration and Development System (JCIDS) manual (ref. JROCM 009-17) that updates the System Survivability Key Performance Parameter (SS KPP). The SS KPP update will encourage requirements developers to leverage the Cyber Survivability Endorsement Implementation Guide (CSEIG) developed by the Joint Staff/J6 in collaboration with the Deputy DoD Chief Information Officer (CIO) for Cybersecurity, the Defense Intelligence Agency (DIA), and the National Security Agency. The CSEIG consists of guidance that helps acquisition programs ensure cyber survivability requirements are included in system designs as early as possible.

For PMs, CDTs, Lead DT&E Organizations, and the cybersecurity T&E community, the importance of this update to the JCIDS manual is directly tied to Phase 1 of cybersecurity T&E, Understand the Cybersecurity Requirements. The SS KPP included in a system’s requirements documents (i.e., Initial Capability Document [ICD], Capability Development Document [CDD], Capability Production Document [CPD], Capability Requirements Document [CRD], Information Systems [IS]-ICD and IS-CDD), is used by the system engineers and system security engineers to define the 10 cyber survivability attributes and risk-managed performance measures in their functional and system requirements documents.

Appendix X1 provides considerations for assessing cyber survivability within the framework of the updated SS KPP.

2.5 DOT&E Cybersecurity Procedures Memoranda

In April 2018, the DOT&E published their revised Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs memorandum to provide revised guidance to the OTAs. The memorandum directs OTAs to perform a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment (AA) of all acquisition programs. Phases 5 and 6 in this guidebook amplify the guidance in the DOT&E memorandum.

In addition, in January 2015, DOT&E published the DBS CEVA memorandum. This memorandum directs OTAs to modify their cybersecurity T&E processes as appropriate for DoD systems whose functions include financial or fiscal/business activities or the management of funds. The memorandum also directs the OTAs to add Cyber Economic Threat Analysis, Cyber Economic Scenario Testing, and Financial Transaction Analysis to their cybersecurity test planning for DBS.
3 Cybersecurity Test and Evaluation Overview

This chapter provides an overview of the six cybersecurity T&E phases and discusses topics that are relevant to all phases.

3.1 Cybersecurity T&E Phases Overview

Figure 3-1 depicts the cybersecurity T&E phases aligned to the DoDI 5000.02 acquisition life cycle. A key feature of effective cybersecurity T&E is early involvement of cybersecurity testers in test analysis and planning. Each cybersecurity T&E phase includes analysis and planning activities for the subsequent phases, starting in Phase 1.

- **Phase 1—Understand the Cybersecurity Requirements.** The purpose of the first phase is to examine the system’s cybersecurity and resilience requirements for developing an initial approach and plan for conducting cybersecurity T&E.
- **Phase 2—Characterize the Attack Surface.** The purpose of the second phase is to identify vulnerabilities and avenues of attack an adversary may use to exploit the system and to develop plans to evaluate the impact to the mission.
- **Phase 3—Cooperative Vulnerability Identification.** The purpose of the third phase is to verify cybersecurity and resilience and identify vulnerabilities and needed mitigations, which will inform system designers, developers, and engineers of needed cyber survivability and resilience improvements to reduce risk.
- **Phase 4—Adversarial Cybersecurity DT&E.** During this phase, an adversarial team tests the system’s cybersecurity and resilience using a mission context and in a cyber-contested operating environment using realistic threat exploitation techniques to identify residual risk.
- **Phase 5—Cooperative Vulnerability and Penetration Assessment.** The purpose of this phase is to fully characterize the cybersecurity and resilience status of a system in a fully operational context and provide reconnaissance of the system in support of AA.

Figure 3-1. Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle
Cybersecurity T&E Phases 1 and 2 are the essential first steps of the T&E planning process that supports system design and development. These two phases define the “who, what, where, when, why, and how” for testing, including the scope of the test, required test tools and infrastructure, and requisite skills of the representative opposing force (OPFOR). Many Program Offices successfully perform Phases 1 and 2 in parallel.

Phase 1 and 2 analyses and planning rely on engagement and collaboration with, and provide feedback to, system engineering (SE) during the early stages of system design and development to facilitate design changes that improve cybersecurity and resilience. SE generates most of the system artifacts, described in Appendix D, required during these analysis and planning phases, and therefore the partnership between SE and the testers is essential.

T&E planning and execution occurs during Phases 3, 4, 5, and 6. Phases 3 and 4 comprise cybersecurity DT&E execution activities for the system. Cybersecurity testers develop test objectives, plan test activities and events, and plan the cybersecurity test infrastructure for Phases 3 and 4 based on the outcomes from the Phases 1 and 2 analyses.

Phases 5 and 6 comprise cybersecurity OT&E activities for the system. Cybersecurity operational testers provide the information needed to resolve operational cybersecurity issues, identify vulnerabilities in a mission context, and describe operational effects of discovered vulnerabilities.

During Operations and Support, PMs should periodically reevaluate systems for cybersecurity and resilience. At a minimum, they should conduct or update a mission-based cyber risk assessment (MBCRA) (see Section 3.6 and Appendix X3) for the system when a significant change to the mission, system, threat, or operating environment occurs. Examples of significant changes include: system modernization efforts, discovery of new threat vectors (zero-day vulnerabilities), or deployment of a system to a new operational environment. The results of the MBCRA activity may drive additional Phase 1 through 4 T&E activities, depending on the changes to mission risk. Even without significant changes to mission, system, threat, or operating environment, PMs should conduct or update the MBCRA for the system, with a focus on RMF continuous monitoring efforts in support of renewing the systems’ ATO. The Life Cycle Sustainment Plan should include cybersecurity T&E.

### 3.1.1 Iterative Nature of the Phases

Cybersecurity T&E phases are iterative (i.e., activities may be repeated multiple times due to changes in the system architecture, new or emerging threats, and changes in the operational environment). For example, when a significant change to the system architecture occurs, such as after a Preliminary Design Review (PDR) or initiation of an Engineering Change Proposal (ECP), the CDT or system test lead usually repeats the first two phases to incorporate any changes that may impact test planning and before conducting Phases 3 through 6 testing. Iteration through the phases supports updates to the TEMP concurrently with SE activities to update requirements, architecture, and design. Figure 3-2 depicts phase iteration after initial testing during Phase 3. Whenever testers verify cybersecurity and resilience, and discover new high-risk vulnerabilities, the PM should update requirements to mitigate the discovered vulnerabilities.
3.1.2 Tailoring Phases

PMs should address the six cybersecurity T&E phases regardless of where the system is in the acquisition life cycle. Figure 3-1 depicts the cybersecurity T&E phases with colors to show their alignment with the acquisition life cycle. The figure represents the cybersecurity T&E phases where there is ample time in the life cycle for all phase activities. Some systems, however, enter the acquisition lifecycle at Milestone (MS) B, incrementally update major components of the system, or are already well into the acquisition life cycle when cybersecurity T&E phases are initiated. Accelerated acquisition programs may not have time for the full progression through the phases as depicted in Figure 3-1; however, the Program Office should devote time to the early analysis that the phases identify to establish the foundation for efficient cybersecurity and resilience testing. Appendix C describes tailoring considerations for cybersecurity T&E phases and provides examples for DBS that use the BCAC, smaller acquisition programs, acquisition programs using alternative acquisition milestones, and acquisition programs with compressed timelines.

3.2 Cybersecurity Working Group

The recommended approach for planning and implementing the phases of cybersecurity T&E is for the CDT or test lead for the system to establish, as early as possible, a Cybersecurity Working Group (CyWG) that reports to the T&E Working Integrated Product Team (WIPT). The CDT or system test lead should ensure the CyWG roles and responsibilities are documented in Section 2 of the TEMP. The CyWG is responsible for integrating and coordinating all cybersecurity T&E and supporting the RMF assessment and authorization (A&A) process. The Information System Security Manager (ISSM) is the focal point for RMF A&A activities, and the remaining members of the CyWG are crucial to ensuring the full range of cybersecurity T&E is planned and executed. The Cybersecurity T&E Lead will guide the test planning for the CyWG. The CyWG performs the tasks in the phases as described in this guidebook: analysis, planning, scheduling, and assessment for all cybersecurity T&E. The CyWG focuses on integrating cybersecurity T&E with functional T&E and assessing mission-based cybersecurity risk to inform the PM before acquisition and engineering decisions.

The recommended minimum participants in the CyWG are:

- CDT or system test lead if the CDT has not yet been appointed
- Systems Security Engineer (SSE)
- ISSM
- Lead Systems Engineer Representative
- Lead Software Engineer/Architect
- Lead DT&E Organization Representative
- Operational Test Agency Representative, if available
- Cybersecurity DT&E Technical Experts (testers/analysts/assessors)
- Cybersecurity OTA Technical Experts (testers/analysts/assessors), if available
Cybersecurity Test and Evaluation Guidebook 2.0

- Security Controls Assessor (SCA)
- Cybersecurity Subject Matter Experts (SMEs)
- Cyber-Intelligence SME
- Cyber Test Range Representative
- Service-Specific T&E Policy Representative, if needed
- Oversight organizations and stakeholders as appropriate
- Prime Contractor, if appropriate

RASCI Matrix. A Responsible, Accountable, Supporting, Consulting, Informed (RASCI) matrix defines the team needed to complete project tasks and their assigned role in each task. Using the recommended roles above, PMs may want to develop a RASCI matrix that supports the cybersecurity tasks described in this guidebook. Appendix F provides an example.

3.3 Cybersecurity Threat Assessments

A cybersecurity threat is an actor or a set of conditions that can cause an adverse mission effect. An assessment of cybersecurity threats should scrutinize each element that may bring about mission performance failures. Designing a system without understanding the relevant cybersecurity threat may result in system weaknesses or exposures that a human or automated process could exploit. It is also important to understand how the system may be used in an unintended manner to cause mission performance failures. The CyWG recommends an appropriate frequency for conducting cybersecurity threat assessments throughout the system development life cycle, but at a minimum, the Program Office receives a validated threat assessment (e.g., Validated Online Lifecycle Threat [VOLT] report or Service/Component threat assessment report) at each acquisition milestone. The Program Office is responsible for evaluating and updating the mission risk assessment and RMF risk assessment if necessary using updated threat assessment information. For a detailed explanation of developing, updating, and using the cybersecurity threat assessment throughout cybersecurity T&E, see Appendix X2.

3.4 DT&E and SE Collaboration

Early and regular collaboration between T&E and SE helps acquisition programs avoid costly, difficult system modifications late in the acquisition life cycle. The CDT or system test lead and SE should collaborate with SE providing architecture and design information and derived critical technical parameters to the CDT. The CDT will use this information to inform T&E activities and scenarios, to include what data to require of the contractor, and to shape government test designs. DoDI 5000.02, Enclosure 14 provides greater detail into the various required cybersecurity activities across the system development life cycle.

SE derives critical technical parameters required for test planning. Figure 3-3 illustrates the typical interaction between cybersecurity T&E activities and SE program protection activities during the traditional acquisition life cycle. Although Figure 3-3 depicts the full acquisition life cycle, this guidebook recommends that PMs determine how to appropriately integrate SE and T&E in the program’s acquisition strategy using the applicable DoD policy and guidance.
Figure 3-3. Interaction of SE and T&E Cybersecurity Activities

T&E and SE should collaborate early to conduct MBCRAs/CTT exercises, described in Appendix X3, to inform the design of a system that will perform its mission in a cyber-contested environment. Early T&E collaboration is important because the contractor will build and test to the requirements only, ensuring that the system meets specifications. During Phase 1 and 2, cybersecurity testers examine cybersecurity mission risk and cybersecurity and resilience requirements to target systems for test activities that the system’s SE and design documents define.

The Program Office system engineers develop the Program Protection Plan (PPP) that describes the program’s critical program information (CPI), mission-critical functions and components, and the expected threats to CPI and mission-critical functions. The PPP describes the plan to apply countermeasures to mitigate risk associated with cyber threats to CPI and mission critical functions only, not other cyber vulnerabilities. Contractor and government testers must verify the effectiveness of the countermeasures.

The CyWG is the body of experts that enables SE and T&E to collaborate on cybersecurity and resilience issues. Integrating the adversarial and vulnerability test teams with the system engineers and developers (via the CyWG) allows the PM to design cyber resiliency into the functional mission resiliency. To inform system designs, system engineers focus on mission capabilities, functional resiliency, safety, and cybersecurity threats. Cybersecurity testers supplement SE knowledge by assessing threats and vulnerabilities inherent to the system designs. Adversarial cybersecurity testing informs SE of the system cybersecurity and resilience posture beyond compliance with implemented cybersecurity controls and configurations.
3.5 Early Tester/Analyst Involvement

The CDT or system test lead should include and engage cybersecurity testers/analysts, including OTAs, vulnerability assessment teams, and Red Teams, shortly after acquisition program initiation and before MS B. During Phase 1, cybersecurity testers analyze architectures, system designs, and key interfaces to expose any additional implied and essential cybersecurity and resilience requirements. Testers also identify the T&E data needed to assess progress toward achieving cybersecurity and resilience requirements.

Early tester/analyst involvement benefits acquisition programs in the following ways:

- Helps shape emerging cybersecurity and resilience requirements, ensuring testable, measurable, and achievable requirements defined through the SE process and critical technical parameters (CTPs).
- Ensures cybersecurity requirements are coordinated through the test chain from integration test to developmental test to operational test.
- Ensures incorporation of cybersecurity T&E requirements into Request for Proposals (RFPs) and Statements of Work (SOWs), including specific cybersecurity and resilience testing tasks and Contract Data Requirements Lists (CDRLs). Appendix B provides additional information for cybersecurity T&E contract recommendations.
- Ensures that cyber survivability and resilience requirements are consistent with the mission and threat conditions.
- Advises PMs and conducts early testing and analysis to identify any systematic cybersecurity and resilience issues; conducts cybersecurity risk analysis, provides timely mitigation recommendations for fixes and verifies fixes which reduces risk of system re-design and modification.
- Identifies cybersecurity and resilience shortfalls and provides mitigation recommendations for vulnerable developmental prototypes to ensure systems are resilient and easier to maintain over time, which reduces system life cycle costs.
- In collaboration with the intelligence community, helps PMs refine relevant cybersecurity threats, establish necessary countermeasures, and structure mission-oriented cybersecurity and resilience requirements for development and testing.
- Ensures early planning for cybersecurity and resilience test infrastructure and plans for long lead times and potentially destructive testing needed for test articles, tools, and facilities.

3.6 Mission-Based Cyber Risk Assessments

Because it is often not possible to address all vulnerabilities, susceptibilities, and exploitable attack paths before a system is fielded, the CyWG plans and conducts an MBCRA beginning in Phase 1 to focus and prioritize the cybersecurity T&E effort. MBCRA is a process for identifying, estimating, assessing, and prioritizing risks based on impacts to DoD operational missions resulting from cyber effects on the system(s) employed. There are many MBCRA methodologies to choose from. Appendix X3 presents several common MBCRA methodologies, such as the CTT exercises, and presents a decision structure to assist acquisition programs with selecting a methodology best aligned to the system’s maturity, Program Office goals and resources, and desired outputs. Recognizing MBCRAs as a best practice and a recommended tool, Section 3.1, Figure 3-1 depicts MBCRAs across the acquisition life cycle with increasing fidelity as the system design matures.

3.7 Role of Cybersecurity Developmental Testing

Cybersecurity DT&E evaluates a system’s mission performance in the presence of cybersecurity threats and informs acquisition decision makers regarding cybersecurity, resilience, and survivability. The focus
of testing is system resiliency; testing assesses if the mission can avoid disruption due to system misuse. The CDT must plan DT&E to verify not only cybersecurity and resiliency capabilities, but also identify mission-impacting cybersecurity vulnerabilities. Cybersecurity DT&E also informs functional testing of the vulnerabilities discovered and identifies exploits that may be used against those vulnerabilities.

Early discovery and assessment of system vulnerabilities can facilitate remediation, reduce mission risk, and reduce impact on cost, schedule, and performance, as well as increase likelihood of a successful operational test and mission effectiveness. Late testing renders system remediation much more difficult due to the pressures of cost and schedule constraints.

Cybersecurity DT&E includes RMF assessment activities to provide a thorough evaluation of the system’s cybersecurity and resilience posture. Cybersecurity DT&E test results inform PMs about the relevance of vulnerabilities affecting mission execution and resilience. DT&E activities also include, for example, design and code reviews, application scanning, penetration testing, and regression testing. Cybersecurity DT&E activities are not one-time activities that provide static information. Organizations must employ ongoing DT&E activities throughout the system development life cycle. The frequency of DT&E activities depends on the defined purpose and scope of assessments required during system development.

**RMF Integration.** RMF A&A is necessary but not sufficient to ensure that a system can operate in a cyber-contested environment. The RMF assessment process assesses if planned security capabilities are in place, but it does not test how well the security capabilities work in the presence of a cyber threat during mission execution. By integrating RMF assessment activities with cybersecurity DT&E, the Program Office completes a thorough evaluation of the system’s cybersecurity and resilience posture and informs decision makers and Authorizing Officials (AOs) about the risks to mission execution. During the test planning process, the ISSM works with the CDT to identify and schedule all cybersecurity test activities.

Early in the process, cybersecurity DT&E verifies all implemented security controls and performance parameters before the formal security controls assessment to ensure controls operate as intended and to implement fixes and verify the fixes. Phases 2, 3, and 4 of the cybersecurity T&E process provide data to SE and the ISSM that may inform and support execution of RMF processes and inform additional, modified, or strengthened countermeasures and controls.

After T&E, test reports apprise the SCA regarding the compliance status of security controls and inform the AO who is assessing risk associated with the results. Figure 3-4 illustrates the integrated timeline of T&E results in a traditional life cycle that inform AO decisions. For acquisition programs following tailored or modified life cycles, as discussed in Appendix C, tailor the RMF alignment to the modified life cycle and cybersecurity T&E.
Figure 3-4. Interaction of RMF and T&E Cybersecurity Activities

See DoDI 8510.01 for more details on RMF and the AO role. For more information about the RMF process integration into the acquisition life cycle, see DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle (see References for more information).

**Interim Authority to Test (IATT).** An IATT is required if an operationally realistic environment or live operational data is required to support functional DT&E or early operational assessments. The CDT and ISSM should include the IATT plan and resources in the TEMP, as part of the cybersecurity T&E plan.

The plan for an IATT includes early cybersecurity contractor and developmental testing, security controls assessment, and assessment of Security Technical Implementation Guide (STIG) compliance. The CDT should plan to conduct verification of controls in developmental labs and isolated test ranges before receiving an IATT as part of the RMF process. Testing conducted using a closed-loop cyber range and cyber range events does not require an IATT and may inform subsequent IATT/ATO decisions. The CDT should review the test objectives for IATT testing and document in the TEMP and detailed test plans:

- The security controls that must be assessed for the IATT.
- The security controls that the contractor must design, develop, and assess for inclusion in the Development RFP.
- The order in which security controls must be designed, developed, and assessed.
- Need for, and timing of, STIG compliance testing.
- Required cybersecurity and resilience testing, to potentially include limited adversarial testing.

The CDT or system test lead coordinates with the PMs to ensure that the contract specifies any contractor testing required for the IATT.

**Integrated Testing and Data Sharing.** The CDT and CyWG develop an integrated cybersecurity T&E strategy that includes cybersecurity DT&E, OT&E, and RMF requirements. To conserve Program Office time and resources, the CDT and CyWG should integrate all testing requirements documented in the TEMP, including contractor assessment and testing activities, into routine test objectives and test plans as early in system development as possible. CDTs should align the TEMP with the system’s cybersecurity strategy in the PPP, the RMF Security Plan, and the Security Assessment Plan.
With proper planning and authorization that includes DT&E, OT&E, and RMF representatives, data reuse can occur during Phase 3 and Phase 5 by providing all data from cybersecurity DT&E and RMF controls assessment to the SCA and AO and OT&E testers. Integrated cybersecurity T&E strategies identify cybersecurity-related data from all available contractor and government sources, including RMF security controls assessments, security inspections, developmental tests in system integration labs, testing in operational environments, and testing with systems and networks that representative end users operate. The collective data set supports comprehensively evaluating the system’s cybersecurity and resilience posture. Programs Offices document and track remediation of all discovered vulnerabilities in a Plan of Action and Milestones (POA&M).

3.8 DT&E and OT&E Collaboration

Cybersecurity OT&E testers are highly encouraged to participate in planning during the early phases of cybersecurity DT&E. When funded by the Program Office, OTAs participate in T&E Phases 1 and 2 as members of the CyWG to gain information about cybersecurity and resilience requirements, mission risks, key terrain, and systems’ potential attack surface. The CDT or system test lead also coordinates with the OTA during Phases 1 and 2 to facilitate test planning if the Program Office will be conducting tailored T&E, integrated T&E, or early cybersecurity OT&E. Section 3.4 discusses tester collaboration with SE. When leveraging a DT&E environment to satisfy OT&E requirements, the OTA must evaluate the emulated operational environment to ensure it is as operationally realistic as possible.

Integrated Cybersecurity T&E. Integrated T&E eliminates duplication of efforts, facilities, personnel, or other resources for cybersecurity testing. Integrated T&E allows test events to share a single test point or mission that can provide data to satisfy multiple objectives, without compromising the test objectives of either the DT&E or OT&E. Integrated planning activities enhance the operational realism in DT&E, providing opportunities for early identification of system design improvements. Integrated T&E does not replace or eliminate the need for dedicated Initial Operational Test and Evaluation (IOT&E), as required by 10 USC 2399, *Operational Test and Evaluation of Defense Acquisition Programs*. For more information about integrated T&E, see Defense Acquisition Guidebook (DAG), Chapter 8. The CyWG identifies opportunities for integrated cybersecurity test events to satisfy DT&E and OT&E test objectives if possible, such as integrating Phases 3 and 5. Conducting cybersecurity OT&E as an integrated exercise with cybersecurity DT&E in an emulated operational environment supports evaluation of destructive threat testing that may be restricted or prohibited in the live operational environment.

Including both Lead DT&E Organization and OTA cybersecurity testers in CTT exercises and other MBCRAs adds valuable operational and adversarial test expertise to the assessment. An MBCRA developed during cybersecurity DT&E and then updated based on OT&E results can help stakeholders make informed, risk-based decisions and helps to prioritize needed remediation to improve system resilience.

If OT&E begins before the ATO, then cybersecurity test results and identified risks/mitigations at the end of OT&E are included in the ATO submission package by the OTA to help inform the decision to approve/disapprove the ATO.

3.8.1 Cybersecurity Evaluation

Test teams plan cybersecurity T&E based on the cybersecurity and resilience information that the PM needs to inform the Decision Support Questions (DSQs) defined in the DEF, evaluate critical technical parameters, and answer the Critical Operational Issues (COIs) described in the OT&E Operational Evaluation Framework (OEF). Appendix E provides additional information about developing the cybersecurity portion of the DEF. The CDT should direct the cybersecurity test teams to conduct a cybersecurity and resilience evaluation after each test event. When a cybersecurity and resilience evaluation follows every test event, the PM is informed about the cybersecurity and resilience of the
system at that point in time. Cybersecurity evaluations, the ‘E’ of DT&E and OT&E, cover the following topics:

- Is the system/software/hardware developed using industry security best practices?
- Do security controls and countermeasures prevent and mitigate malicious activities as intended?
- Can mission-critical cybersecurity assets withstand cyber-attacks and intrusions?
- Do exposed vulnerabilities adversely affect system resiliency?
- Can the system adequately recover from cyber-attacks and intrusions?
- Do information and diagnostic tools provided to system operators function correctly to enable satisfactory identification, response, and recovery actions?

Cybersecurity evaluations include a cybersecurity risk assessment that describes operational mission impacts from cyber-attacks, which informs the system authorization decisions. The CyWG leads cybersecurity evaluations and facilitates obtaining test data from cybersecurity test teams to answer the evaluation questions. Section 3.2 describes CyWG participation.
Phase 1: Understand Cybersecurity Requirements (and Plan for T&E)

Most DoD systems operate in cyber-contested environments. The purpose of Phase 1 is to understand the system’s cybersecurity and resilience requirements defined through the SE process for operating in cyber-contested environments and to develop an initial approach and plan for conducting cybersecurity T&E. Phase 1 analysis uses engagement and collaboration with system engineers and operators to facilitate design changes that improve resilience. For Phase 1 to be successful, SE and the CDT or system test lead should collaborate closely. Enclosure 14 of DoDI 5000.02, paragraph 5.b.(10), describes Phase 1 of cybersecurity T&E and the analysis and collaboration that takes place as part of SE activities to plan and prepare for T&E. The process for Phase 1 is the same for all acquisition programs, and Appendix C provides guidance on tailoring. Figure 4-1 shows Phase 1 inputs, key tasks, and outputs. Appendix A provides a quick-look table of the tasks. Appendix F depicts a sample RASCI breakdown of the tasks.

4.1 Schedule

Understanding cybersecurity and resilience requirements is key to the T&E planning process. Gaining an understanding of these requirements should occur as early as possible in the acquisition process, preferably before MS A or when initiating system modification efforts. If a system is moving toward MS C and has not previously conducted cybersecurity T&E phases, then the Program Office should begin with a review of the cybersecurity and resilience requirements before it moves through each cybersecurity T&E phase. If no cybersecurity or resilience requirements are specifically called out in requirements documents, they can be derived using the process described in Table 4-1.

Phase 1 analysis is an iterative process, as depicted in Figure 4-2 and discussed in Section 3.1.1. Phase 1 extends into the Engineering and Manufacturing Development (EMD) phase of the acquisition life cycle, specifically because of the variety of acquisition programs and the reality of changing requirements throughout early phases of the life cycle. For DBS, assessment of cybersecurity requirements should be performed when new functionality is released because the new functionality may change the cybersecurity posture of the DBS.
4.2 Inputs

The following system artifacts, outlined in Appendix D, are the inputs needed to gain an understanding of cybersecurity and resilience requirements:

- Capability Requirements Documents: JCIDS ICD, CDD, or Capability Production Document (CPD)
- Cyber Survivability Risk Category from CSEIG process
- DBS System Functional Requirements
- PPP including Criticality Analysis, Supply Chain and Anti-Tamper requirements, and Cybersecurity Strategy (DoD or Component CIO approved document)
- SE Plan
- DoDAF System Views
- DBS Design Specifications (if available)
- DBS Capability Implementation Plan (if available)
- VOLT report, Cyber Threat Modules (CTMs) from the Defense Intelligence Threat Library (DITL)
- RMF Security Plan, RMF Security Assessment Plan
- MBCRA, if available
- Previous cybersecurity vulnerability assessment reports, penetration testing reports or AA reports, if available

Although these documents will be in various stages of completion early in the development cycle, the CDT or system test lead should include even incomplete documents in the requirements list. Program Offices can update this information as documents are updated.

4.3 Tasks

The CDT or system test lead initiates and convenes the CyWG, as described in Section 3.2, as early as possible to assist with the tasks described below.

4.3.1 Compile List of Cybersecurity and Resilience Requirements

As early and as often possible, the CyWG reviews system documentation to extract: 1) cybersecurity and resilience requirements; 2) information that may influence test conditions, environments, or methods; and 3) information that may influence the prioritization of testing. The CyWG ensures that the requirements are testable, measurable, and achievable. Appendix X1 describes considerations for developing measures for cybersecurity testing. The documents listed as inputs in Section 4.2 provide information on the requirements and testing factors found in Table 4-1.
### Table 4-1. Cybersecurity and Resilience Requirements and Testing Factors to Consider

<table>
<thead>
<tr>
<th>Requirements/Test Factors</th>
<th>Description</th>
<th>Why?</th>
<th>Where to Find</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission operation in cyber-contested environments</td>
<td>Sets general expectations for operations in a cyber-contested environment.</td>
<td>Derive cybersecurity and resilience requirements from this statement to ensure required mission operation.</td>
<td>JCIDS Documents TRDs</td>
</tr>
<tr>
<td>Cyber survivability attributes of the system survivability KPP</td>
<td>Attributes categorized as (1) Prevent; (2) Mitigate; and (3) Recover.</td>
<td>Attributes provide specific cybersecurity requirements evaluated via T&amp;E. If absent, refer to SE for resolution.</td>
<td>JCIDS Documents</td>
</tr>
<tr>
<td>System KPPs, KSAs</td>
<td>SE derives a level of cybersecurity controls/countermeasures from an analysis of KPPs / Key System Attributes (KSAs).</td>
<td>Test the effect of cyber-attacks on performance thresholds.</td>
<td>JCIDS Documents</td>
</tr>
<tr>
<td>System critical components and information</td>
<td>Select and implement countermeasures to protect CPI, functions and components.</td>
<td>Critical components and information point to potential prioritization within T&amp;E activities.</td>
<td>PPP/Criticality Analysis appendix</td>
</tr>
<tr>
<td>Software testing</td>
<td>The PPP defines testing that must occur to ensure security of development items.</td>
<td>Describes software developmental items and requirements for testing them.</td>
<td>PPP</td>
</tr>
<tr>
<td>Anti-tamper (AT) requirements</td>
<td>The PPP defines AT activities to protect CPI via system architecture design including hardware and software techniques.</td>
<td>Describes deter, impede, detect, and response countermeasures to CPI exploitation in DoD systems. Countermeasures should be used to design test activities if needed.</td>
<td>PPP/AT Plan appendix</td>
</tr>
<tr>
<td>Security requirements and engineering specifications</td>
<td>SE translates higher level security requirements into engineering specifications.</td>
<td>Use these specification details as required to design T&amp;E activities for specific components and subsystems.</td>
<td>TRDs</td>
</tr>
<tr>
<td>Network and information architectures</td>
<td>Identifies system under test (SUT) critical data exchanges and interfaces.</td>
<td>Informs test infrastructure planning—data exchanges and interfaces are part of the attack surface and may require testing.</td>
<td>Information Support Plan (ISP); DoDAF System Views</td>
</tr>
<tr>
<td>Cyber-Electronic Warfare (EW) operations</td>
<td>Cyber-EW implications of new, existing or modified waveforms on mission operations; Cyber-EW dependencies inform cybersecurity requirements</td>
<td>Testing needs to consider waveforms as a cybersecurity threat vector; cyber-EW testing informs test infrastructure planning.</td>
<td>Waveform Assessment Application, for more information, see References</td>
</tr>
<tr>
<td>Cyber threat assessment</td>
<td>Intelligence reports provide information on adversary cybersecurity objectives, targets and capabilities, including cyber-attack techniques, tactics and procedures. Use the cybersecurity threat assessment to design countermeasures.</td>
<td>Test countermeasures to ensure that they protect the system to withstand the threat. This information shapes T&amp;E of attack surfaces and the corresponding countermeasures and defensive techniques. Threat adversary emulation drives test infrastructure planning.</td>
<td>VOLT report, CTMs, DITL Service-specific Threat Assessment Report</td>
</tr>
<tr>
<td>RMF controls</td>
<td>Security controls are specific methods used to achieve cybersecurity goals.</td>
<td>Consider RMF controls during test planning.</td>
<td>RMF Security Plan</td>
</tr>
<tr>
<td>RMF security controls assessment</td>
<td>Details the schedule and methodology for assessing security controls implementation.</td>
<td>Consider assessment plan during test event scheduling ensuring controls are implemented before to testing.</td>
<td>RMF Security Assessment Plan</td>
</tr>
</tbody>
</table>

---

**Phase 1: Understand Cybersecurity Requirements**
<table>
<thead>
<tr>
<th>Requirements/Test Factors</th>
<th>Description</th>
<th>Why?</th>
<th>Where to Find</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSSP</td>
<td>The CSSP provides layers of cybersecurity monitoring and defense.</td>
<td>Testing, particularly in operationally realistic environments, needs to take into account the layers of monitoring and security that the CSSP provide.</td>
<td>PPP/Cybersecurity Strategy appendix</td>
</tr>
<tr>
<td>Financial system requirements if applicable</td>
<td>DoD financial systems may contain cyber economic vulnerabilities and cyber economic SMEs must ensure the key operational capabilities and business processes are evaluated.</td>
<td>Financial systems are required to conduct a CEVA IAW DoDI 5000.02 and 5000.75.</td>
<td>JCIDS Documents TRDs</td>
</tr>
<tr>
<td>Cybersecurity risk categorizations</td>
<td>The Joint Staff’s CSRC and the DoD CIO RMF Categorization.</td>
<td>The depth and breadth of cybersecurity T&amp;E strategy should reflect the cybersecurity risk to the systems that these risk categorizations describe.</td>
<td>JCIDS Documents RMF Security Plan / Cybersecurity Strategy</td>
</tr>
<tr>
<td>MBCRA results</td>
<td>If available, identifies the current cyber risk posture for the system.</td>
<td>Current risk posture of the system drives further T&amp;E planning and focus to reduce risk.</td>
<td>MBCRA Document</td>
</tr>
<tr>
<td>Supply chain protection requirements</td>
<td>The PPP defines supply chain risks and how the program will manage risks to critical functions and components</td>
<td>Describes how supply chain threat assessments are used to influence system design and development environment.</td>
<td>PPP/Supply Chain Risk Management Section</td>
</tr>
</tbody>
</table>

Additional cybersecurity and resilience requirements are implied or derived from system characteristics (e.g., operation on a public network, technology choices such as operating systems or commercial-off-the-shelf (COTS), system access methods). Appendix G presents considerations for planning and performing software assurance testing. The CyWG should consider all requirements when planning cybersecurity testing.

### 4.3.2 Prepare for Cybersecurity T&E Events

**Develop the Initial DEF.** The DEF, included in the TEMP, guides development of the DT&E strategy by identifying the critical acquisition program decisions and defining the test data needed to inform the decisions. Understanding system performance requirements in the context of cybersecurity and resiliency is essential to determine cybersecurity T&E events and data required to inform the DSQs. Appendix E explains the tasks needed to develop the cybersecurity portion of the DEF and provides examples of cybersecurity and resilience test activities that could be included within the DEF. When developing the cybersecurity portion of the DEF, the DEF Core Team, with support from the CyWG, uses the DEF Core Team defined DSQs to perform the tasks. The DAG, Chapter 8 and the TEMP Guidebook (see References) provide additional details on the DEF.

**Identify Supporting Cybersecurity T&E Resources.** To support the collection of the necessary cybersecurity test data, the CDT or system test lead, in collaboration with the CyWG, identifies the labs, ranges, tools and personnel that will support cybersecurity T&E activities. The CyWG uses threat information to design the threat actions used against the system during testing and to identify organizations that can portray those threats. Adversarial Cybersecurity DT&E (ACD) assessment teams and infrastructures such as ranges and labs require scheduling well in advance. In some cases, the government may have resourced the contractor to develop T&E Infrastructure such as a Systems Integration and Test Lab that could be used by the government for cybersecurity T&E. The CyWG may want to carefully plan and coordinate with the contractor to ensure the contractor test infrastructure can also be accessed and used by the government for cybersecurity T&E. The CDT or system test lead
includes the ACD testing events in the overall T&E schedule. Early identification and scheduling of cybersecurity test teams is key to ensuring their availability when needed. See Appendix F and Appendix X4 to assist with identifying resources.

**Develop the Initial OT Evaluation Framework.** For the OT Evaluation Framework, the TEMP includes measures for cybersecurity and resilience as part of operational test plans. DOT&E and/or the OTA 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.

**Align RMF Activities with the TEMP.** The CDT or system test lead coordinates with the ISSM to align the development of the RMF Security Assessment Plan with the pre-MS B decisional TEMP delivery. The TEMP must reflect RMF activities and include a schedule of controls assessment and resources required for controls assessment in addition to describing the cybersecurity T&E planning activities and tests that will occur in in Phases 1 through 6.

**Plan and Schedule an MBCRA.** An MBCRA, such as a CTT exercise, examines stated, implied, and essential cybersecurity and resilience requirements; the cybersecurity risks the system may face; and possible impacts on mission operations. See Appendix X3 for more information.

### 4.3.3 Plan for Cybersecurity T&E

**Develop Cybersecurity T&E Strategy.** The cybersecurity T&E strategy documented in the TEMP includes RMF assessment activities and thoroughly explains the following for every planned testing activity. Depending on the system’s phase, details of each activity may not be available in the current TEMP:

- Who will perform the testing (contractor, Lead DT&E Organization, vulnerability test team or adversarial assessment team, etc.)?
- What will be tested (software, component, subsystem, etc.)?
- Where the testing will occur (range, labs, contractor facility, distributed, etc.)?
- Why the testing is planned (controls assessment, architecture assessment, adversarial assessment, CTT verification, vulnerability assessment, etc.)?
- When the testing events will occur (frequency if repeated), including MBCRA events?
- How the testing will be conducted (tools, infrastructure, resources, threat, etc.)?
- How execution of cybersecurity test activities and events will provide data for evaluations?
- How remediated or mitigated vulnerabilities will be retested to verify removal of the vulnerability?
- How the evaluations will provide decision makers with essential information about the cybersecurity and resilience of the system?

The strategy must explain how test organizations will carry out the cybersecurity T&E activities, including attack surface characterization, vulnerability identification, and adversarial assessments, in accordance with the CSTE six-phase process.

### 4.4 Outputs

- List of cybersecurity and resilience requirements and other factors that influence cybersecurity testing.
- Inclusion of cybersecurity T&E items within the system Development RFP: Who, what, where, when, why, and how for contractor required cybersecurity T&E. More information about contractor cybersecurity T&E language is contained in Appendix B.
- Updates to MBCRA (as needed).
4.4.1 TEMP Updates

The CDT or system test lead updates the MS A, MS B, and MS C TEMPs with Phase 1 information after every iteration. When developed early, the MS A TEMP will lack the detail of the MS B TEMP, but must show that thought is given to the cybersecurity risks that the system will face, the measures that the system is taking to mitigate those risks, and the T&E that is necessary to assess how well the system implements those cybersecurity and resilience measures. Include the following items:

- Cybersecurity T&E Strategy incorporating cybersecurity T&E Phases 1 through 6
  - Include the plan for cyber-attack surface characterization, vulnerability identification (contractor and government), penetration testing, and adversarial assessments
- Initial Developmental and OEFs as described above.
- Plans and schedule for cybersecurity test activities and integrated required RMF activities.
- Identification of cybersecurity T&E resources—funding, personnel, ranges, tools, etc.

4.4.2 Acquisition Reviews and Decisions Informed by T&E

Activities during Phase 1 inform the following acquisition reviews and decisions:

- **MS A Risk Reduction Decision.** Provide input into developing Analysis of Alternative. Testers provide T&E inputs for each alternative developed. MBCRAs performed on alternatives are useful in evaluating cybersecurity risk. Use the criteria, issues, COIs, CTPs, measures of effectiveness, and measures of suitability developed for these documents to develop the strategy for T&E and subsequent T&E plans for the selected alternative.
- **Prototype Development Decision.** Evaluate prototypes, architectures, new technologies; demonstrate prototypes meet mission needs in cyber-contested environments.
- **CDD.** Assess if the cybersecurity and resilience requirements are testable, measurable, and achievable in both the draft and final CDD.
- **Solution Analysis Authority to Proceed (ATP) and Functional Requirements ATP.** For DBS under DoDI 5000.75, Phase 1 analysis informs both Solution Analysis and Acquisition ATP decisions.
- **MS B RFP and Contract Award.** Provide input to the RFP that details required contractor cybersecurity T&E activities. See Appendix B for additional information.
- **PDR.** Consider providing a preliminary DT&E analysis in support of the PDR based on any testing that has occurred and the testing planned to date. A DT&E analysis will likely be more thorough after completion of Phase 2.
5 Phase 2: Characterize the Cyber-Attack Surface

In this phase, the CDT or system test lead schedules and conducts activities to identify mission-critical components, data, and known vulnerabilities, and how an adversary may gain access. Enclosure 14 of DoDI 5000.02 paragraph 5.c.(5) describes the Phase 2 analysis and collaboration that takes place as part of SE activities to examine cyber threats to prepare for T&E.

Phase 2 ideally starts before EMD, occurs during technology maturation and risk reduction (TMRR), and continues into EMD. However, a Program Office would perform this phase wherever the system enters the acquisition life cycle after or in parallel with Phase 1. Phase 2 analysis is an iterative process as shown in Figure 5-2; Program Offices revisit this phase before a major milestone or for any changes to the system’s attack surface or threat profile. Attack surfaces change throughout the development and testing cycles. Once ACD assessments begin, there may be additional and more likely attack vectors and

5.1 Schedule

Cyber-Attack Surface

The different points in a system architecture where an attacker could gain entry to compromise a system. The system’s exposure to reachable and exploitable vulnerabilities (i.e., any connection, data exchange, service, removable media, etc., that could expose the system to potential threat access).
vulnerabilities identified. Previous test results and remediation of test findings inform attack surface analysis and support refinement of the attack surface during each stage of testing.

![Figure 5-2. Phase 2 Iteration](image)

**5.2 Inputs**

The following system artifacts are inputs for characterizing the cyber-attack surface. Appendix D further describes key artifacts for T&E analysis.

List of cybersecurity and resilience requirements assembled in Phase 1:

- CONOPS, CONEMP, User manuals
- DBS Capability Implementation Plan
- DBS Capability Support Plan (if available)
- CSSP support plan
- Information Support Plan (ISP)
- DoD Architecture Framework (DoDAF) operational views (OVs) and system views (SVs)
  - OV-1: High-Level Operational Concept and other operational views as needed
  - SV-1: Systems Interface Description
  - SV-2: Systems Resource Flow Description
  - SV-6: Systems Resource Flow Matrix
- DBS Design Specifications
- System Design Documents
  - Contractor system designs
  - Wiring diagrams
  - Logical and physical network architecture diagrams
- System Interface Control Document
- Lists of system hardware and software
- RMF Security Plan and Security Assessment Plan
- Authorization boundary diagrams including systems and data flows
- PPP
  - Criticality Analysis
  - Software assurance testing requirements
  - Mission-essential functions and dependencies
- System Threat Assessment
  - System-relevant cybersecurity threats, including technological threats and assumed threats
  - VOLT report, CTMs, DITL
  - Service/Component Cyber Threat Intel (CTI)
  - Publicly available CTI
- System Engineering Plan (SEP)
- TEMP
  - DEF
5.3 Tasks

The CyWG performs the tasks identified for Phase 2.

5.3.1 Identify the Cyber-Attack Surface

To characterize the cyber-attack surface, the CyWG first identifies all forms of communication, network connectivity, software, hardware, and human interaction and creates an attack surface list to use when identifying key cyber terrain and potential attack vectors. System architecture products, such as the SV-6, aid in this identification. In addition, the CyWG analyzes and decomposes the mission that the system performs to support follow-on attack surface analysis. The CyWG also identifies critical components and data (key terrain) that support mission essential functions. These are not the only potential attack surfaces, but rather are the known attack vectors.

Note that the RMF Security Plan and systems security engineering efforts also examine the system architecture and may provide information on the cyber-attack surface. The subtasks listed below will guide the CyWG efforts toward completing this task. The example in Table 5-1 illustrates an attack surface list for a notional mobile navigation system.

<table>
<thead>
<tr>
<th>System Component</th>
<th>Interfaces</th>
<th>Information Exchanges</th>
<th>Data</th>
</tr>
</thead>
</table>
| GPS Receiver     | • GPS antenna  
                              • Fiber interface  
                              • Serial port       | • GPS navigation messages (GPS antenna)  
                              • Navigation messages (Decryption module)  
                              • Configuration updates (factory)    | • Navigation data (encrypted, in transit)  
                              • Configuration data (at rest)         |
| Decryption Module | • Fiber interface  
                              • Ethernet interface  
                              • Serial interface    | • Navigation messages (GPS receiver)  
                              • Navigation messages (Processing module)  
                              • Key management information (Key custodian)  
                              • System administration commands (Admin)    | • Navigation data (decrypted, in transit)  
                              • Cryptographic algorithm (at rest)  
                              • Cryptographic keys (at rest)          |
| Processing Module| • Ethernet interface  
                              • Serial interface    | • Navigation messages (Decryption module)  
                              • Enriched mission information (Geolocation tagging unit)  
                              • Navigation messages (Geolocation tagging unit)  
                              • Storage information (Storage module)    | • Navigation data (at rest)  
                              • Maps (at rest)  
                              • Enrichment data (at rest)  
                              • Mission data (at rest)          |
| Storage Module   | • Ethernet interface  
                              • Removable media drive | • Storage information (Processing module)  
                              • Archive download (Analyst)  
                              • Maintenance commands (Database manager)    | • Navigation data (at rest)  
                              • Mission data (at rest)         |
| Geolocation Tagging Unit | • Ethernet interface  
                              • Fiber interface | • Enriched mission information (Processing module)  
                              • Navigation messages (Processing module)  
                              • Mission and navigation information (Platform)  
                              • Mission and navigation information (Encryption module)  
                              • Maintenance commands (admin)    | • Navigation data (at rest)  
                              • Mission data (at rest)  
                              • Access control information (at rest)          |
| Network Switch   | • Ethernet interface  
                              • Wireless interface | • Configuration updates (admin)    | • Navigation data (in transit)  
                              • Mission data (in transit)  
                              • Configuration data (at rest)         |
<table>
<thead>
<tr>
<th>System Component</th>
<th>Interfaces</th>
<th>Information Exchanges</th>
<th>Data</th>
</tr>
</thead>
</table>
| Encryption Module | • Fiber interface  
• Serial port | • Navigation and navigation messages (Geolocation tagging unit)  
• Navigation and mission information (Radio Frequency (RF) transmitter)  
• System administration commands (Admin) | • Navigation data (encrypted, in transit)  
• Mission data (encrypted, in transit)  
• Cryptographic algorithm (at rest)  
• Cryptographic keys (at rest) |
| RF Transmitter | • Fiber interface  
• RF antenna | • Navigation and mission information (Encryption module)  
• Navigation and mission information (Command and control system) | • Navigation data (encrypted, in transit)  
• Mission data (encrypted, in transit) |

Steps for examining system architecture, components, and data flows:

- Use system design documents, logical and physical network diagrams, ISP, and DoDAF views to refine the attack surface list so that it contains interfacing systems and data connections that may expose the system to potential threats.
- Identify the points of entry/exit into the system by examining where external systems/software/hardware interact with the system hardware, software, and firmware, even if limited or temporary.
- Examine and include interfaces that are used as well as those not used for normal system functionality.
- Use CONOPS, CONEMPs, and other documentation for users (operators and defenders, if applicable) or maintainers to understand how people will use, maintain, interact with systems.
- Use the RMF Security Plan to identify host environment provisions (controls) for system protection, monitoring, access control, system updates, etc. Common controls have known attack surfaces. Specialized controls may introduce new attack surfaces, and additional controls or procedures (countermeasures) may need to be included in the system design or CSSP responsibilities.
- Some systems may have fault trees that identify probability and likelihood of faults and failures through a failure mode, effects, and criticality analysis (FMECA). If SE has conducted a FMECA for the system, the data can supplement system design information.

Inputs to identify:

- Direct network connections (see current DoDAF products and contractor design documents)
- Indirect DoD network connections—where the system connects to a trusted system with direct network connections, including air-gapped or removable media and administrator interfaces.
- Temporary connections and built-in connections not intended for use: maintenance processes and/or devices, storage devices used to upload new software, maintenance ports, enabled physical, and logical ports
- EW interfaces to cyber components
- Data inputs and outputs
- Supply chain interactions (see PPP)
- Authentication methods
- Applications and software
- Ports, protocols, and services
Phase 2: Characterize the Cyber Attack Surface

- Human accesses, including users with higher privileges
- Manufacturer connections/accesses
- Default settings
- Where data is encrypted, decrypted, inspected, manipulated, stored, and shared.
- Security measures provided or required by the host enclave or CSSP

**Analyze and Decompose System Mission.** The CyWG examines the system CONOPS, CSSP support plan, and additional systems documentation to analyze the mission and link to mission-critical functions. This analysis includes the roles and responsibilities of system operators, defenders, system administrators, and the CSSP and includes maintenance processes for potential additional attack surface entry points. The CyWG updates the attack surface listing with potential insider attack surface points and identifies all human interaction with hardware, software, and firmware.

**Map Mission Dependencies.** The CyWG uses the PPP criticality analysis and CONOPS to map the mission dependencies at the component, system, and mission thread level to the attack surface and identify attack paths. This includes identifying critical components and data (key cyber terrain) that support mission-critical functions. This mission decomposition, shown in Figure 5-3, will help in the next task, Analyze the Attack Surface.

The result is a criticality overlay on the mission decomposition and attack surface list to use in the next task. The overlay should clearly identify in the attack surface list:

- Critical technology, components, and information (key cyber terrain)
- Mission-essential functions (MEFs)
- Operational procedures and workarounds

---

**Figure 5-3. Example Mission Decomposition and Criticality Analysis**

---

Phase 2: Characterize the Cyber Attack Surface
The final output of this task is a list or diagram that identifies and relates system missions, MEFs, components, communication paths, insider areas of concern, attack paths, and mission-essential nodes or exposures. Figure 5-4 illustrates a cyber-attack surface, in the form of a system diagram, for this same notional mission system that is ready for analysis.

![Notional Mobile Navigation System Diagram](image)

**Figure 5-4. Example Cyber-Attack Surface System Diagram**

### 5.3.2 Analyze the Attack Surface

For each military mission that the system supports or business function that it performs, the CyWG analyzes the identified attack surface’s likely avenues of cyber-attack and identifies opportunities an attacker may use to exploit the system. The goal is to prioritize areas of the attack surface, based on mission impact and threat characterization (mission risk), for Phase 3 and 4 cybersecurity T&E. The CyWG also looks for relationships between functional T&E and the attack surface and paths. MBCRAs are the recommended approach to complete this task, and NIST 800-30 identifies three approaches for risk analysis: threat-oriented, asset/impact-oriented, or vulnerability-oriented. Appendix X3 describes various MBCRA methodologies generally aligned to the three approaches and how a PM might decide which methodology to use.

Phase 2: Characterize the Cyber Attack Surface
Characterize the Cyber Threat. The CyWG uses the system’s current threat intelligence to determine if the expected threat adversary has the current or indicated potential motivation and capability to access the system and exploit mission-critical functions as identified in the attack surface analysis.

The CyWG develops a threat profile, incorporating known cybersecurity adversary objectives, resources, and techniques, tactics and procedures (TTPs) and evaluates the threat likelihood in terms of difficulty of attacks. This helps prioritize the attack surface list, to document the desired threat representation for testing, determining, and prioritizing the adversary's desired mission-based effects. The threat profile includes:

- System-relevant cybersecurity threats
- VOLT report, CTMs, DITL
- Service/Component Cyber Threat Intelligence (CTI)
- Publicly available CTI

The CyWG updates the threat profile with additional information as needed to support an ongoing understanding of the attack surface. Threats will evolve and new vulnerabilities will become known in the future. For additional information on using cyber threat assessments during cybersecurity T&E, see Appendix X2.

Select a Cyber Kill Chain. The cyber kill chain is a framework for describing a broad range of activities that a cyber attacker may undertake when conducting an offensive against a target system. The cyber kill chain organizes these activities into phases into an attack sequence. While a cyber kill chain is not a precise recipe for a cyber-attack, applying the cyber kill chain framework to perform an attack path analysis for a system under test is helpful to determine how to improve the system’s resiliency. Figure 5-5 is an example of a cyber kill chain and includes brief descriptions of the four main phases—prepare, gain access, propagate, and affect—and two cross-phase activities—command and control and reconnaissance.

Examine Cyber Effects on the System and Mission. The CyWG explores cybersecurity adversarial TTPs targeting the cyber-attack surface and determines attack paths that can have mission impact using, among other things, results from Phase 1 to understand what cybersecurity and resilience capabilities are in place across the attack surface. Factors making an attack surface more susceptible to compromise may include supply chain risk, attack surface accessibility/exposure, insider threats, and the technical capabilities required to use different avenues of attack. The CyWG should also pay special attention to exploits and paths that can result in impacts to critical components and critical information and should refer to the Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), National Vulnerability Database, and Common Attack Pattern Enumeration and Classification (CAPEC) websites (see References) to cross-reference the identified attack surface list with known vulnerabilities and typical cyber-attacks.
The CyWG uses a cyber kill chain, the attack surface list (e.g., Table 5-1), the mission decomposition and criticality analysis (e.g., Figure 5-3), the cyber-attack surface system diagram (e.g., Figure 5-4), and the system threat assessment to conduct an attack path analysis and to develop a prioritized cyber-attack surface diagram as represented for the notional system in Figure 5-6. The difference between this figure and the previous is the prioritization of the attack surface to use in planning for follow-on cybersecurity T&E. Attack surface diagrams are often developed during an MBCRA (e.g., CTT exercise) from the perspective of an adversary trying to attack the mission-critical functions. The MBCRA also identifies other potential system vulnerabilities that should be included in the cyber-attack surface analysis.
The CyWG documents exploitation techniques that can lead to an impact on an asset at every step in the cyber kill chain as well as known or needed countermeasures or mitigations for each exploit. The CyWG should understand the cybersecurity requirements that protect the key terrain and the resiliency requirements that enable mission essential functions to continue while a system is under attack. The CyWG should also document testing tools, infrastructures, and environments necessary to verify and validate cybersecurity and resiliency of the system in a mission context.

**Perform (or Update) Mission-Based Cybersecurity Risk Assessment.** The CyWG selects an MBCRA methodology to evaluate the mission risk and inform a prioritized risk-based testing approach for Phases 3 and 4. Appendix X3 describes MBCRA methods. The assessment also includes determining the likelihood of every identified exploitation technique, which comprises the threat capability and required level of effort as well as many attributes of the attack surface and path vulnerabilities. Evaluate the impact of the exploitation on the mission to include the perspective of system operators and defenders. The likelihood and impact assessments will result in a prioritized risk assessment. Use the MBCRA to generate a prioritized list of attack surface areas of concern for Phase 3.

### 5.3.3 Document Results and Update Test Planning and Artifacts

**Document Results of Cyber-Attack Surface Analysis in a Cyber-Attack Surface Analysis Report.** The CyWG documents the identified cyber-attack surface list, the critical components and data (key terrain) that support mission essential functions, the analysis of the attack surface, any known vulnerabilities, and the recommended activities, such as attack surface testing, mitigation design, risk acceptance, and requirements, for further analysis. The resulting Cyber-Attack Surface Analysis Report specifies updates needed for the roles and responsibilities, system design, and system cybersecurity and resilience requirements. Note that the RMF process and systems security engineering efforts also examine the system architecture and may provide information for this analysis. The CyWG shares the report and all supporting documentation with SE, the Program Office, CDT, cybersecurity testers, and stakeholders.
5.3.4 Prepare for Phase 3 and Phase 4 Cybersecurity DT&E Events

The analysis in Phase 2 informs the CDT and OTA on appropriate threat level, threat tactics, user/operational considerations, and testing tools needed to support DT&E and OT&E adversarial testing in a mission context. At this point in the cybersecurity T&E process, primary responsibility shifts to the test community, with support from the SE community, to define the test strategy. The attack surface analysis is a planning and tracking tool to track what needs testing, what was tested, and what will not be tested.

Formulate Test Strategy. The CyWG plans a series of Phase 3 and/or Phase 4 activities that will evaluate the areas of concern identified in the previous tasks and inform the acquisition program decisions as identified in the DEF. Specific events to consider:

- Additional MBCRA or similar exercises
- Contractor test events and use of contractor system integration labs
- Compliance assessments of system components with all applicable STIGs and technical specifications in SE documents
- DT/OT collaborative test planning effort
- Interoperability testing
- Integration of component testing
- Software testing
- Architecture vulnerability assessment
- Network vulnerability assessment
- Functionality of RMF controls in the integrated system
- Platform and component hardening verification
- Adversarial testing in a mission context

Schedule. The overall T&E schedule includes the ACD testing events; ACD assessment teams and infrastructures such as ranges and labs require scheduling well in advance.

5.4 Outputs

The characterization of the cyber-attack surface provides input into subsequent test planning and supports updates to roles and responsibilities (including the CSSP support plan), SE design, and requirements. The following products should be produced at the end of this phase and used to update the TEMP and inform acquisition reviews and decisions:

- Attack surface analysis report which includes:
  - An attack surface list
  - Mission decomposition and criticality analysis
  - Attack surface analysis (e.g., prioritized attack surface diagram and list)
- List of interfacing systems and data connections that may expose the system to potential threats
- List of known vulnerabilities in the system as identified in the tasks above, and those identified through the RMF process (as documented later in the RMF POA&M, if available)
- Identified attack surface protection responsibilities and gaps or areas of concern
- Cybersecurity T&E resource requirements
- Updated MBCRA

5.4.1 TEMP Updates

The CyWG updates the MS A TEMP if developed and updates the MS B and MS C TEMPs with Phase 2 information after every iteration. The MS B TEMP should show that the testers understand cybersecurity

Phase 2: Characterize the Cyber Attack Surface
risks the system will face, the measures the system is taking to mitigate those risks, and the required T&E to assess how well the system implements those cybersecurity and resilience measures.

The cybersecurity T&E Strategy (who, what, where, why, when and how), including resources to align with the test strategy—funding, personnel, ranges, tools, etc., should now include:

- Addressing the results of the cyber-attack surface characterization, vulnerability identification (contractor and government), and adversarial assessments
- Refining test strategy for Phase 3
  - Tools, skills required
  - Test environment
  - User, CSSP, or organic defensive cyber operations (DCO), interface representation
  - Schedule
  - What contractor testing will be performed
  - Integrated testing
  - Risks associated with areas not planned for testing
- Updating DEF and OEFs as described above

5.4.2 Acquisition Reviews and Decisions Informed by T&E

Activities during Phase 2 inform the following acquisition reviews and decisions:

- **CDD Validation.** Assess whether the cybersecurity and resilience requirements are testable, measurable, and achievable in both the draft and final CDD.

- **MS B RFP, Contract Award, Functional Requirements ATP (for DBS under DoDI 5000.75).** Provide input to the RFP that details required contractor cybersecurity T&E. See Appendix B for additional information.

- **PDR, Functional Requirements ATP and Acquisition ATP (for DBS under DoDI 5000.75).** Cybersecurity DT&E assesses the maturity of cybersecurity and resilience design features used to detect cybersecurity threat activity, react to cybersecurity threat activity and restore mission capability after degradation or loss. The CDT or system test lead may consider providing a preliminary DT&E analysis in support of the PDR or Acquisition ATP (for DBS under 5000.75) decision based on any testing that has occurred and the testing planned to date.

- **CDR.** Cybersecurity DT&E re-assesses maturity of cybersecurity and resilience design features used to detect cybersecurity threat activity, react to cybersecurity threat activity, and restore mission capability after degradation or loss.
PROGRAM TIP: “The value of executing Phase 2, Characterizing the Cyber-Attack Surface, is that it enables cybersecurity testers to develop efficient tests. For example, our program executed a CTT event to characterize the attack surface with a mission focus. The follow up analysis of the attack surfaces identified seven high mission impacting attack vectors, three medium risk attack vectors, and 12 low risk attack vectors that could not be identified using scanning tools. The CDT Officer and the cybersecurity test lead were then able to work with a cyber range to plan and develop a CVI Test event (Phase 3) to determine if the high-risk attack vectors were technically feasible and to further analyze the medium risk vectors. The program implemented mitigations early to address the verified mission impacts. This process gave focus to the CVI with achievable test objectives to inform product development. This focused test used our programs limited resources efficiently.”
The Cooperative Vulnerability Identification (CVI) phase, which Enclosure 14 of DoDI 5000.02 and DoDI 5000.75 require, consists of detailed planning and execution of cybersecurity vulnerability testing. The purpose of Phase 3 is to identify known cybersecurity vulnerabilities in hardware, software, interfaces, operations, and architecture; to assess the mission risk associated with those vulnerabilities; and to determine appropriate mitigations or countermeasures to reduce the risk. The CDT evaluates contractor test data against SE-defined critical technical parameters to verify that the system as operationally fielded meets the stated capabilities. The vulnerability assessment team assesses vulnerabilities and provides feedback to system designers and engineers to resolve discovered vulnerabilities. The vulnerability assessment team may also perform cooperative penetration testing to improve system resilience. Phase 3 activities are cooperative in that the attack surface documented during Phase 2 informs the Phase 3 vulnerability assessment team efforts. Vulnerability testing during CVI also focuses on discovering vulnerabilities in COTS and government-off-the-shelf (GOTS) systems, software, and hardware.

Figure 6-1 shows Phase 3 inputs, key tasks and outputs. Appendix A provides a quick-look table of the tasks. Appendix F depicts a sample RASCI breakdown of the tasks.

Figure 6-1. Phase 3: Cooperative Vulnerability Identification Activities

CVI is not a single test event. The CDT plans and conducts test activities designed to test, analyze, fix, and retest the components, subsystems and systems throughout development, as shown in Figure 6-2. CVI follows a testing continuum that integrates formal and informal test events tailored for each system. CVI events conclude with a cybersecurity evaluation that assesses the status of all discovered vulnerabilities (remediated and/or mitigated), current and anticipated threats, and risks to mission operations.
Phase 3: Cooperative Vulnerability Identification

Figure 6-2. Phase 3 Testing Process

The PM uses CVI test results to inform DEF DSQs, as described in Section 3.8.1 and Appendix E, and to inform the PPP and Security Plan. CVI results may include security controls assessment results for the IATT request. When possible, CVI should include penetration testing. Phase 3 testing lays the foundation for successful Phase 4 ACD by identifying known vulnerabilities in the system components, interfaces, hardware, firmware, and software. Many COTS components contain known vulnerabilities that are exploitable as documented in vulnerability databases, such as the CWE, CVE, National Vulnerability Database (NVD) and CAPEC (see References). CVI testing mitigates known component and software vulnerabilities.

6.1 Schedule

CVI planning begins before MS B for acquisition programs under the DoDI 5000.02 or after the Authority to Proceed decision for DBS under DoDI 5000.75. The CDT documents the plan in the MS B TEMP or the DBS implementation plan documentation. CVI test execution begins at MS B and includes contractor T&E activities. Vulnerability testing results from CVI provide input to the CDR as well as data to inform the acquisition decisions documented in the system’s DEF. Since DoDI 5000.02 policy requires Phase 3 PMs must plan for and conduct Phase 3 testing activities regardless of when the system enters the acquisition life cycle. Phase 3 test execution is an iterative process, as depicted in Figure 6-3, where the test, analyze, fix, and retest process is conducted until all known vulnerabilities have been remediated. The schedule should allow time for final mitigation of known vulnerabilities prior to Phase 4 ACD. For information on tailoring Phase 3, refer to Appendix C.

Figure 6-3. Phase 3 Iteration

6.2 Inputs

The following system artifacts are inputs to Phase 3. Appendix D further describes key artifacts for T&E analysis.

- Cybersecurity portion of the DEF
- Attack Surface Analysis Report from Phase 2
- Test results from contractor T&E activities
- Test results from component-level testing
- Software Requirement Specification

Phase 3: Cooperative Vulnerability Identification
6.3 Tasks

The CDT has the lead role for cybersecurity test planning, execution, and reporting during Phase 3.

6.3.1 Plan CVI Test Activities

The CDT and CyWG, including the vulnerability assessment team and threat testers, plan contractor and government tests to focus on potentially vulnerable functions in components, interfaces, and architecture that are critical or essential to mission operation success. Phase 1 and 2 analyses, along with the cybersecurity portion of the DEF, provide prioritized information about system architectures, interfaces, and components and their relationship to mission operations. Note that the bulk of test planning takes place before Phase 3, and the ATO decision takes place after ACD testing in Phase 4.

Whenever possible, the CDT plans to test in a mission context to demonstrate system resiliency. Testing in a mission context means using the mission CONOPS, representative mission data, emulated interfaces, user representatives including operators, maintainers, and defenders, and mission threads/vignettes to test (when possible) and to evaluate the test results during Phase 3.

The CVI test scope includes the system of systems (SoS) environment, to include the following components as discovered during Phase 2:

- SUT
- CSSP-inherited protections (may need to emulate during CVI)
- Critical data exchanges
- Critical interfaces to mission systems that may introduce attack vectors
- Vulnerabilities discovered through the RMF process as available.

An important goal of test planning is to design tests that produce repeatable, defensible test results that effectively support decision makers. Scientific Test and Analysis Techniques (STAT) are essential to achieving these goals. STATs are scientific and statistical methods with associated processes used to enable the development of efficient, rigorous test strategies. For more information on STAT, see the DAG, Chapter 8-3.7.4.

Develop Cybersecurity Test Objectives. The CyWG develops cybersecurity test objectives to guide test planning and align with the critical technical parameters. Test objectives describe the desired outcomes from test activities, along with measures that demonstrate improvement as SUT development progresses. Table 6-1 shows example evaluation goals, test objectives, and metrics based on CSEIG cybersecurity attributes (CSAs) supporting an assessment of Prevent, Mitigate and Recover (PMR). PMs must test the survivability attributes associated with PMR during CVI and assess PMR during Phase 4 using a CSSP if possible.
### Table 6-1. Example Evaluation Goals, Test Objectives and Metrics

<table>
<thead>
<tr>
<th>Example Developmental Goals</th>
<th>PMR/CSA</th>
<th>Example Test Objectives</th>
<th>Example Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>System monitors the cybersecurity configuration baseline for cyber anomalies in real time by:</td>
<td><strong>Prevent</strong>&lt;br&gt;CSA 3: Reliable, Confidential Transmissions and Communications&lt;br&gt;CSA 4: Protect System’s information from exploitation</td>
<td>Determine the system’s susceptibility to cyber-attacks.&lt;br&gt;Examine integrity and confidentiality of critical-mission data.&lt;br&gt;Ensure cryptographic devices are operating as intended.</td>
<td>Percent of malicious code detected in tested software.&lt;br&gt;No unauthorized software is resident on operational system.</td>
</tr>
<tr>
<td>• performing malicious code protection;&lt;br&gt;• intrusion detection using automated tools for real-time analysis;&lt;br&gt;• information system monitoring;&lt;br&gt;• security alerts;&lt;br&gt;• security function verification;&lt;br&gt;• software, firmware, and information integrity;&lt;br&gt;• incident monitoring, handling, reporting, and response</td>
<td><strong>Mitigate</strong>&lt;br&gt;CSA 7: Monitor System and Detect Anomalies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System detects and discards malformed messages and invalid inputs.</td>
<td><strong>Prevent</strong>&lt;br&gt;CSA 4: Protect System’s information from exploitation</td>
<td>Verify: System validates data inputs for mission related data.</td>
<td>Percent of tested malformed and invalid inputs blocked/dropped.</td>
</tr>
<tr>
<td>System takes active measures to identify and deny unauthorized access attempts to include denial of service (DOS) and distributed DOS, at the system, its internal boundaries, and cross-domain interfaces with other systems.</td>
<td><strong>Prevent</strong>&lt;br&gt; CSA-01: Control Access&lt;br&gt; CSA-04: Protect System’s information from exploitation</td>
<td>Verify: Access control denies access to unauthorized connections and user/process interactions&lt;br&gt;Unauthorized attempts are identified and denied&lt;br&gt;Effectiveness of internal and external boundary defenses.</td>
<td>Percent of tested unauthorized access attempts are deflected.</td>
</tr>
<tr>
<td>System degrades gracefully (e.g., quality of service) before degrading to unacceptable mission consequences</td>
<td><strong>Mitigate</strong>&lt;br&gt; CSA-8: Manage System Performance if degraded by cyber events</td>
<td>Verify: System maintains minimum performance required to prevent adverse mission consequences.</td>
<td>System degradation falls within acceptable mission performance thresholds.</td>
</tr>
<tr>
<td>Software patches and updates are authenticated using digital signatures and vendor-approved techniques.</td>
<td><strong>Mitigate</strong>&lt;br&gt; CSA 10: Manage System Patches and Vulnerabilities</td>
<td>Verify: Patch process authenticates all software patches and system updates prior to initiating the patching process.&lt;br&gt;Percent software patches and system updates authenticated before patch initiation.</td>
<td></td>
</tr>
<tr>
<td>System provides automated tools to authenticate, deploy, and verify the success of patches and software updates and that security baselines have not been unintentionally altered, whether patches and software updates were deployed on local or remote components.</td>
<td><strong>Mitigate</strong>&lt;br&gt; CSA 10: Manage System Patches and Vulnerabilities</td>
<td>Verify: Patch and vulnerability management effectiveness, including timeliness for pending patches and critical patches.</td>
<td>Percent of critical patches deployed within the required timeframe.</td>
</tr>
</tbody>
</table>
**Plan and Schedule Test Events.** The CDT plans and prioritizes cybersecurity testing based on test events and test data needed to resolve test objectives and verify the system capabilities. The attack surface informs the analysis to ensure key cyber terrain is thoroughly tested throughout cybersecurity T&E. The CDT also plans CVI testing to ensure the vulnerability assessment teams have all the levels of system access required to successfully assess for common exploitable vulnerabilities. The CDT identifies common vulnerabilities that can arise in systems, configurations, and across interfaces that system developers or the PM were not aware existed.

The CDT plans for a continuum of CVI activities scheduled throughout development. Early in system development, CVI testing focuses on software, hardware components, and subsystems that the contractor performs. CVI activities include contractor cybersecurity T&E activities during Phase 3 starting at MS B. The earliest developmental test activities are contractor T&E activities supporting contractor development efforts. The scope of contractor cybersecurity test activities informs the scope of government T&E activities. Government testers must evaluate contractor test data against CTPs (defined as part of the SE process) to verify that the system meets the stated capabilities. Phase 1 and 2 inform the RFP to clearly state the testing requirements, CTPs, CDRLs supporting cybersecurity T&E, and test data contractors are responsible for producing. Appendix B provides additional information about cybersecurity T&E contract language considerations. A major aspect of contractor T&E involves software assurance testing. Appendix G presents considerations for software testing.

During integration of platforms and components, the CDT should plan testing events to conduct CVI across interfaces (interoperability), with emphasis on critical data exchanges and interfacing systems with critical mission impact. Testing should continue until a full-up system is completely tested.

When possible, later developmental testing also includes penetration testing. Later in development, prior to ACD and after the system has entered government DT&E, the CDT should plan to conduct testing in a simulated mission context, with representative users (operators and defenders as appropriate), to assess mission resiliency to cyber-attacks. The Program Office should track vulnerabilities and mitigation efforts; at a minimum, the CDT should plan to verify fixes on mission-critical components, planning time to fix systems and retest before scheduling the next test activity. Table 6-1 below describes example developmental vulnerability test activities to plan and conduct during CVI. The CDT tailors and selects tests that align with system test data requirements including vulnerability test activities in the developer’s contract.

**Test Plan Documentation.** The TEMP documents planned tests using detailed test plans. Testing of functions critical to mission success are prioritized in test plans to ensure that they are not vulnerable to cyber-attack. Test planners scope the tests to describe how they will conduct the testing and on what specific systems, users, data exchanges, and interfaces. The test plan details test limitations or special cases that will require unique treatment. The test schedule includes dates, times, and estimated duration of test events. The plan specifies the quantity and details of all required resources (cybersecurity SMEs, tools, contractor development labs, cyber ranges, users, etc.) or data (previous testing). For more information on test plans, see the DAG, chapter 8–3.6.4 T&E Plans. The planned testing activities, such as the examples in Table 6-2 dictate the expectations for the test conductor skills. For example, an Oracle expert would not be expected to test a non-IP based system. Use Appendix F to help select the appropriate test resources for the various planned test activities.
## Table 6-2. Example Test Activities

<table>
<thead>
<tr>
<th>CVI Test Activities</th>
<th>Description</th>
<th>Test Conductors</th>
<th>Test Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architectural Vulnerability Assessment (AVA)</strong></td>
<td>Examines network and system architecture attributes that may introduce attack paths to critical cyber assets.</td>
<td>System architect, system security engineer</td>
<td>Examine contractor technical design documentation. Investigate inherent architectural vulnerabilities. Examine trust relationships external to the SUT and critical data exchanges.</td>
</tr>
<tr>
<td><strong>Software Testing</strong></td>
<td>Identifies and eliminates software errors and vulnerabilities in critical components; contractor T&amp;E is the earliest instance of software testing.</td>
<td>Contractor software tester Government software tester</td>
<td>Perform software security verification using requirements specified in the PPP. Address three areas: 1) Software development environment 2) Software development processes 3) SUT operational software For more information, see Appendix G.</td>
</tr>
<tr>
<td><strong>Network Vulnerability Assessment</strong></td>
<td>Targets SUT’s enclave network boundary, internal networks, system interfaces, network security components.</td>
<td>Government network engineer</td>
<td>Test for misconfigured devices and nonfunctional protections at the network level, such as network segmentation and firewalling.</td>
</tr>
<tr>
<td><strong>Cybersecurity Functionality Verification</strong></td>
<td>Verifies cybersecurity functionality to ensure that security controls and countermeasures are working as intended in a mission context.</td>
<td>Security controls assessor Cybersecurity tester</td>
<td>Test security controls and countermeasures in a mission context before IATT. Verify contractor cybersecurity T&amp;E results.</td>
</tr>
<tr>
<td><strong>Platform and Component Hardening Verification</strong></td>
<td>Verifies security of components and platforms at the supply chain and hardware levels.</td>
<td>Vulnerability tester</td>
<td>Platform and component hardening verification provides input to the SE process. Assess patching processes for components to address vulnerabilities that occur after deployment.</td>
</tr>
<tr>
<td><strong>Developmental STIG Verification</strong></td>
<td>Rigorous component scanning that includes evaluating scan results, eliminating false positives, performing manual checks.</td>
<td>Vulnerability tester</td>
<td>Test each critical cybersecurity asset and adjudicate all confirmed findings. Use multiple scanning tools to cross-validate vulnerability findings. Note: STIG verification during DT&amp;E provides input to AO and does not replace RMF SCA.</td>
</tr>
<tr>
<td><strong>CTT Exercise Verification Test</strong></td>
<td>Provides actionable information to PMs about mission impact of vulnerabilities discovered during CTT exercises.</td>
<td>CTT exercise Opposing Force (OPFOR) team</td>
<td>Test suspected exploitable vulnerabilities to validate CTT exercise findings. Evaluate system performance during cyber-attack using safe test environments.</td>
</tr>
<tr>
<td><strong>System Misuse/Abuse Testing</strong></td>
<td>Examines how systems are used that are unplanned, unintended or unexpected.</td>
<td>Government penetration testers</td>
<td>Use misuse/abuse scenarios to guide testing with a mission context. An understanding of predicted cybersecurity threats provides input into system abuse scenarios.</td>
</tr>
<tr>
<td><strong>Cyber Survivability Testing</strong></td>
<td>Ensures that mission functions can survive cyber-attacks.</td>
<td>Government security testers</td>
<td>Refer to the CSEIG for more information.</td>
</tr>
<tr>
<td>CVI Test Activities</td>
<td>Description</td>
<td>Test Conductors</td>
<td>Test Considerations</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>Authorized, simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system’s features and data.</td>
<td>Penetration testers and adversarial testers</td>
<td>Target key cybersecurity and resilience assets supporting mission-essential functions for penetration and exploitation.</td>
</tr>
<tr>
<td>Testing Non-IP Devices</td>
<td>Verify security of embedded systems and platforms at the supply chain and hardware levels.</td>
<td>Test engineers specializing in Supervisory Control and Data Acquisition systems, 1553 bus, Controller Area Network (CAN) bus testing</td>
<td>Appendix X5 discusses considerations for testing embedded systems and non-IP devices.</td>
</tr>
</tbody>
</table>

**Plan Cyber Test Infrastructure.** During CVI, vulnerability assessment teams assess potential vulnerabilities using cybersecurity test ranges, contractor test labs, and Service-specific test facilities to better understand impacts of cybersecurity threats to mission operations. The CDT plans and schedules cybersecurity test infrastructure to support test events and test data needed to resolve test objectives, and notes the use of contractor test facilities for the earliest developmental test activities. Appendix X4 provides additional information regarding test facilities and resources. Table 6-3 shows candidate test facilities correlated with cybersecurity DT&E test activities.

**Table 6-3. Cybersecurity DT&E Activities and Cybersecurity Test Facilities**

<table>
<thead>
<tr>
<th>DT&amp;E Test Activities</th>
<th>Test Facilities</th>
<th>Example Cyber Test Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and Software Development Test</td>
<td>Contractor or government system development labs</td>
<td>Phase 3 – Hardware and Software Development Testing</td>
</tr>
<tr>
<td>Component and Subsystem Test</td>
<td>Contractor or government system integration labs</td>
<td>Phase 3 – Platform and Component Hardening</td>
</tr>
<tr>
<td>System Integration Test</td>
<td>Contractor or government system integration labs</td>
<td>Phase 3 – Cyber Functional Verification, Vulnerability Assessments</td>
</tr>
<tr>
<td>Operationally Relevant Test</td>
<td>Government HWIL facilities, cyber ranges</td>
<td>Phase 4 – Adversarial Cybersecurity Developmental Test (ACD), CTT Verification Testing</td>
</tr>
</tbody>
</table>

High-fidelity operational environments often impose restrictions on cybersecurity testing, even during CVI. Earlier testing in simulated operational or development environments with operator/defender involvement (as appropriate) allows for more rigorous testing before OT and should be performed during DT&E. Cyber ranges and HWIL facilities provide more realistic environments while minimizing risk to operational networks. For additional information, refer to Appendix X4.

Phase 3: Cooperative Vulnerability Identification
**Integrated System Testing.** Integrated system cybersecurity testing includes, as much as possible, full-up system mission/functional testing with user involvement and tests cybersecurity and resilience along with specified performance capabilities to address the following questions:

- Can feature misuse impact functional performance?
- Can an exploited vulnerability drive performance outside of required performance thresholds or required timing?

The CDT plans and resources for disposable test articles as needed to support destructive cybersecurity testing of critical cybersecurity and resilience assets, as well as baseline system performance before conducting cybersecurity testing. Baselining may include compromise hunting where forensics experts examine the system, components, software, etc., for malicious code, backdoors, or other evidence of prior intrusions or existing intrusions before cybersecurity testing.

### 6.3.2 Conduct CVI Events and Document Results

Vulnerability assessment teams conduct CVI test events, which include contractor test activities, between MS B and MS C. The CDT provides CVI event reports to the OTA and oversight organizations.

**Obtain Reports.** The CDT receives results of all CVI testing in separate reports that identify technical and nontechnical vulnerabilities, at that point in time. Vulnerability assessment teams verify the implementation of all mitigations and correction of every deficiency in critical mission components before the next test event and prior to adversarial testing. The CDT documents in test reports all vulnerabilities discovered during CVI, including non-remediated vulnerabilities. Program Offices track remediation in the system POA&M to inform the ATO and other acquisition program decisions. Reuse test data from the security controls assessment when possible to supplement cybersecurity DT&E data. Test results provide updated input to the cybersecurity kill chain analysis for Phase 4. Cyber kill chain analysis examines applying countermeasures to the system to raise the level of effort that an adversary must employ to attack the system. Cybersecurity testers should perform cyber kill chain analyses during CTT exercises as a method to determine potential cyber-attacks, impacts, and mitigations. CVI reports describe results of CVI analysis, recommended corrective actions for the system, and corrective actions deferred.

**Cybersecurity Evaluation.** Cybersecurity testing during CVI is a risk reduction activity that results in a cybersecurity evaluation. Section 3.8.1 discusses cybersecurity evaluations.

**Update Mission-Based Cyber Risk Assessment.** Cyber risk assessments prioritize mitigations for action to improve a system’s security posture. An MBCRA/CTT conducted during Phase 3 helps PMs understand suspected mission impacts and prioritize remediation of vulnerabilities based on mission impact. Prioritization also informs funding decisions that drive redesign and remediation during system development. Cybersecurity risk assessments should include contractor T&E test data. Appendix X3 describes methods for conducting an MBCRA.

### 6.3.3 Prepare for Phase 4 Adversarial Cybersecurity DT&E Event

The completion of Phase 3 includes finalizing infrastructure planning for the ACD event(s) performed in the next phase. Issues to consider include system technology maturity, classification, closed-loop testing, infrastructure, user involvement, and data collection. Appendix X4 further discusses considerations for Phase 4 test facility planning. The following questions may aid Phase 4 test planning activities:

- What exploitable vulnerabilities remain?
- What are the likely TTPs an adversary might use to gain access to the system?
Phase 3: Cooperative Vulnerability Identification

- What operational activities or data can the adversary impact when it gains access to a system?
- Do the CSSP, SUT, SoS, or interfacing systems have additional essential cybersecurity and resilience requirements to mitigate operational impacts of documented vulnerabilities and predicted adversary activities?

The CDT should identify test opportunities in which representative systems and services will be available to conduct dedicated adversarial cybersecurity testing in an SoS context during Phase 4 testing. ACD assessment teams and infrastructures such as ranges and labs require scheduling well in advance. The overall T&E schedule must include ACD testing events.

6.4 Outputs

- Formal CVI reports and associated cybersecurity evaluations
- Evidence that known system vulnerabilities are either remediated or enumerated and tracked
- Planning for at least one ACD event performed in the next phase, which may include a Test Readiness Review (TRR)
- Verification of T&E infrastructure requirements for Phase 4, ACD
- Updated MBCRA of system vulnerabilities based on Phase 3 T&E results to inform Phase 4 planning and acquisition decision events

6.4.1 TEMP Updates

The CyWG updates the TEMP to describe the system’s approach to conducting Phase 3, including Phase 1 and 2 analysis inputs and identify and explain the incorporation of specific CVI test events into overall test planning. The TEMP must document CVI cybersecurity test events and map them to the decisions in the DEF as needed.

The CDT aligns the developmental test schedule to integrate RMF and CVI activities as needed and provides a schedule for CVI test events, including the estimated duration. The CDT also specifies the resources required to complete cybersecurity testing, including cybersecurity SMEs, tools, contractor development labs, cybersecurity ranges, and Service-specific test infrastructure. The CDT includes in the TEMP plans to inform CDR and TRR decisions based on test results.

6.4.2 Acquisition Reviews and Decisions Informed by T&E

The system DEF describes the CVI event data that informs specific acquisition program decisions:

- **CDR.** Cybersecurity DT&E re-assesses maturity of cybersecurity and resilience design features used to detect cybersecurity threat activity, react to cybersecurity threat activity, and restore mission capability after degradation or loss based on test results obtained during Phase 3.

- **Functional Requirements ATP, Acquisition ATP, Limited Deployment ATPs.** Cybersecurity DT&E events and associated cybersecurity and resilience evaluations will inform each limited deployment ATP for DBS under the DoDI 5000.75.

- **IATT and ATO.** Cybersecurity DT&E provides test data to the SSE and ISSM for inclusion in the RMF processes. Test data informs the AO regarding compliance status of security controls.
PROGRAM PHASE 3 EXPERIENCE: “We had scheduled a comprehensive CVI event a few months before the ACD event because the expectation was that we were ready to get our ATO paperwork submitted. We scheduled IOT&E the following year. The CVI event discovered vulnerabilities that our controls assessment activities and security/configuration verification activities for our A&A package had not identified. The PM deemed the CVI findings to be too risky to proceed into ACD without remediation. As a result, we postponed the ACD event to allow the developers time to correct the deficiencies in the design. This did not require a contract revision, but there was cost associated with sliding the schedule. Our developer provided the program with a comparative cost for both the cost to correct the vulnerabilities with the schedule slip and the cost to correct the vulnerabilities after IOT&E, essentially when we were fielding the capability. It would have cost the program significantly more to delay the fixes and the AO would have disapproved the ATO with the vulnerabilities not mitigated.”
Phase 4: Adversarial Cybersecurity DT&E

Adversarial Cybersecurity DT&E (ACD), required by Enclosure 14 of DoDI 5000.02 and DoDI 5000.75, includes evaluations of a system’s resiliency in a mission context, using realistic threat exploitation techniques, while in a representative operating environment. The ACD assessment team uses methods typical of cybersecurity threat adversaries described in system threat assessment documents. As part of adversary emulation, the ACD assessment team should explore all available exploits to system resiliency.

The goal of ACD is to verify cybersecurity and resiliency requirements and discover previously unknown, critical vulnerabilities and to determine their mission impact by fully exploiting the system in a safe operational test environment. The key to a successful ACD event is realistic threat and operational environment representations including user (operator and defender) participation. The ACD test infrastructure should allow the flexibility to alter, compromise, and corrupt targeted systems and then restore them to their original operating conditions to ensure a comprehensive assessment of the system resilience to cyber-attack.

Before conducting ACD events, the CDT should ensure that planned remediation of previously discovered vulnerabilities (from Phase 3) is complete and verified with testing. In some cases, remediation of all vulnerabilities prior to ACD is either not feasible or required. Share residual vulnerabilities with the ACD team. Figure 7-1 shows Phase 4 inputs, key tasks, and outputs. Appendix A provides a quick look table of the Phase 4 tasks. Appendix F depicts a sample RASCI breakdown of the tasks.

Figure 7-1. Phase 4: Adversarial Cybersecurity DT&E Activities

7.1 Schedule

The CDT plans for this phase during Phases 1 and 2, document the planned events in the integrated test schedule and TEMP, and refine the plan and schedule as needed during Phase 3. The CDT conducts ACD events before MS C and before the ATO to inform production and ATO decisions and as part of significant functional releases. CDTs should allow enough time to mitigate vulnerabilities found during the ACD before Phase 5. Early ACD events may also inform CDR if performed early enough (recommended). The CDT must plan a TRR before each ACD scheduled. For information on tailoring Phase 4, refer to Appendix C. The Service/Component evaluation agency may evaluate the ACD to
support acquisition decisions. The MDA also conducts an independent assessment of the ACD to support acquisition decisions for MDAPs.

7.2 Inputs

Some or all the following are inputs to ACD test events:

- Cyber threat assessment
- Kill chain analysis
- Cyber-attack surface analysis
- VOLT report, CTMs, DITL, or Service/Component threat assessment
- Verification of cybersecurity T&E infrastructure requirements from Phase 3.
- All cybersecurity test results to date, including RMF assessment results; note: if known system vulnerabilities have not been corrected or mitigated from CVI events, then PMs should evaluate the rationale for continuing with the ACD
- Mature and stable system baseline
- CONOPS, CONEMP, User documentation
- MBCRA

7.3 Tasks

The CDT has the lead role for cybersecurity test planning, execution, and reporting during ACD and works with the CyWG to complete the tasks described below. The ACD assessment team consists of adversarial testers, Red Teams, test planners, and test infrastructure planners. The Service-specific roles defined for the ACD assessment team are included in the RASCI matrix.

7.3.1 Update Cyber Threat Assessment and Attack Surface Analysis

The ACD assessment team reviews the cybersecurity threat assessment and attack surface analysis using the cyber kill chain to identify updates to current threat tactics and targeting. The cybersecurity threat assessment informs the ACD assessment team about how to emulate the expected cybersecurity threat during testing. The cyber kill chain analysis and threat assessment contribute to development of threat vignettes, possible response scenarios, and mitigations used in test planning.

As part of this phase, the CDT and ACD assessment team may obtain updated VOLT reports that include system-specific CTMs from the DITL, and Service-specific intelligence reports to validate developed threat vignettes. See Appendix X2 for more details on using cybersecurity threat assessments for cybersecurity T&E.

7.3.2 Plan Adversarial DT&E

The CDT coordinates with the ACD assessment team to develop a detailed test plan using the updated cyber threat assessment and attack surface analysis in test plan development. The CDT goal is to complete each ACD event test plan within six months of the scheduled TRR. Planning for ACD tests includes the activities described below.

Schedule. ACD assessment teams and infrastructures such as ranges and labs require scheduling well in advance; the overall T&E schedule includes the ACD testing events.

Develop Test Objectives. Test objectives support an evaluation of the system’s resiliency in a mission context, using realistic threat exploitation techniques, while in a representative operating environment. Test objectives should demonstrate system resiliency in the face of validated cyber threats. One way to evaluate system resiliency is to include the DCO team during ACD events and to perform a preliminary assessment of the system’s ability to protect the system from cyber intrusions and threats, detect threat
activity, react to threat activity, and restore mission capability degraded or lost due to threat activity. The preliminary assessment of PMR demonstrates how survivable or resilient the system is in response to cyber-attacks and malicious activities.

**Define metrics.** The CDT clearly defines the test data that needs to be collected during the ACD event that supports cybersecurity and resilience measures. See Appendix X1 for considerations of cybersecurity and resilience measures for T&E. The CDT must ensure test metrics are aligned to the test objectives and that the testing teams are capable of collecting the desired test data.

**Identify resources.** The CDT considers the following resources and costs when planning for ACD events:

- System configuration in a stable environment (hardware and software) on which to perform testing
- Personnel requirements to support testing—tester skills aligned to systems to be tested
- Necessary training for operators and defenders if used during testing
- Licensing for specialized testing tools
- Impact/dependency on existing services
- Network availability and bandwidth (as applicable)
- Tools and equipment for the assessment
- Developing and maintaining a test infrastructure
- Using a test infrastructure that belongs to the contractor or other organization

**Develop rules of engagement (ROE).** The PM and ACD assessment team develop and document in the test plan the ROE and the scope of the assessment before the event. This agreement may involve legal counsel and CSSP to consider all legal and technical provisions. The ROE will generally provide the assessment team with flexibility during testing (not tied to a specific script) while it still operates within a rule set agreed to by all parties. The team will share its ROE with all parties and will describe its threat portrayal based on its knowledge of designated attack vectors and the information provided by the Program Office. Although the ROE will vary depending on the organization performing the assessment, typical pre-conditions required are:

- Definition of all legal procedures, including restrictions related to classified networks and systems
- Appropriate authority for destructive testing
  - Bounds and limitations that the infrastructure owner dictates
- Stable system and network environment
- Restoration procedures including responsible parties for restoration
- A trusted agent to observe the activity and halt it if required
- Understanding of the system mission on the part of the test team

**Define process and test cases.** As developmental test events, the ACD events explore configuration settings and operator workflows to optimize cybersecurity and resilience defenses—a limited test-fix-test methodology. Some identified vulnerabilities will require more significant changes to resolve. The CDT resolves shortfalls identified in each ACD event before proceeding to the next ACD event and before OT&E.

**Plan integrated tests.** When combining cybersecurity test objectives with other test objectives (e.g., interoperability), consider that cybersecurity testing, particularly intrusive, corrupting, or destructive testing, can have an impact on achieving other testing objectives. Note: Destructive testing is not always required. The detailed test plan and ROE should explicitly describe agreements about destructive/nondestructive testing.

**Document test plans.** The CDT, in collaboration with the ACD assessment team, will formally document detailed ACD test plans that describe:

Phase 4: Adversarial Cybersecurity DT&E
• Test objectives
• Test data that will be collected
• System(s) under test
• Test methods
• Testing timeline
  – Time between test runs to make minor configuration changes
  – Sequencing of destructive testing to minimize test interruptions needed for restoration
• ROE
• Test environment
  – All interfaces
  – Description of what components are emulated, live, virtual, or constructive
• Threat portrayal that will be used (See Appendix X2 for more details on cyber threat portrayals for T&E).
• Threats resulting from interfaces and business partner connections
• Specific attack vignettes
• Likely targets, such as critical components
• Resources for resolution of findings or restoration of the system or infrastructure

For more information on test plans, see the DAG, Section 8, Section 3.6.4.

**Finalize preparation of test infrastructure.** The CDT ensures that the ACD test infrastructures, based on the verified requirements identified in Phase 3, are ready to support the upcoming ACD events. Ideally, the infrastructure will allow the flexibility to alter, compromise, and corrupt the targeted systems and then restore them to their original operating conditions within a short time (to allow multiple test runs). Flexible and restorable test environments ease restrictions in the ROE. The less flexible the environment, the tighter the ROE will be, resulting in less effective and less thorough cybersecurity testing.

The CDT schedules cybersecurity ranges and test infrastructures at least 12 months in advance, and works with the range event designers in advance to develop or acquire the needed infrastructure. If the ACD event supports cybersecurity OT&E objectives or integrated DT&E and OT&E, then the OTA must also be involved in the test infrastructure planning.

As much as possible, the CDT plans to perform ACD events in an emulated Department of Defense Information Network (DoDIN) (if the system will interoperate with the DoDIN) in a separate enclave. Any adversarial testing taking place on the actual DoDIN traversing between the DoDIN and the internet will require a National Security Agency (NSA)-certified and U.S. Cyber Command (USCC)-accredited Red Team and an IATT or ATO, with more restrictive ROE for the testers.

The CDT coordinates with the ACD assessment team to ensure that the environment is suitable for the testing planned and that tools are available for gathering the test data for assessment. Appendix X4 provides additional information regarding the infrastructure and environment planning.

**Conduct TRR for ACD.** The CDT presents the test objectives, test methods, and procedures, the scope of tests, and ROE during the TRR. The CDT will also confirm identification and coordination of required test resources, including the infrastructure, to support planned ACD tests.

### 7.3.3 Conduct Adversarial Cybersecurity DT&E and Document Results

**Perform ACD events.** The ACD assessment team uses methods typical of cybersecurity threat adversaries (as described by system threat documents) to expose vulnerabilities, and documents the results in an evaluation report. The CDT includes the DCO team during ACD events if possible to perform a preliminary assessment of PDRR/PMR capabilities of the system and system operators and defenders.
**Obtain reports.** The test team report describes vulnerabilities discovered in system components, the team’s assessment of possible impacts to mission operations, and recommended corrective actions. The CDT provides information to update the RMF POA&M, if needed, with ACD test findings requiring corrective actions and uses ACD test results to inform updates to the PPP and Security Plan. The CDT also provides ACD reports to the OTA and oversight organizations.

The CDT may use test activity logs as training material for the DCO team. The test activity demonstrates what cyber-attacks look like from a network detection perspective. The results can be used to practice detection capabilities and to update detection operating procedures.

Recommended corrective actions may not be limited to the SUT, but may extend to the host enclave and CSSP and may include:

- TTP changes
- Configuration changes too extensive to adjust during the event
- Software or hardware modifications

**Cybersecurity evaluation.** Section 3.8.1 discusses cybersecurity evaluations. During ACD events, the test team may be able to directly show what the mission impacts are from exploited vulnerabilities. If the test team is unable to fully execute an attack due to test limitations and ROE, further study such as an MBCRA/CTT, may be required (by system engineers, testers, operator/defender representatives, and security experts) to estimate what the adversary might be able to accomplish. The CDT uses the ACD report to inform deficiency reporting and acquisition program decisions based on actual and estimated mission impacts. The cybersecurity evaluation may include a preliminary assessment of PDRR/PMR.

**Exit Criteria for Cybersecurity DT&E.** The CyWG establishes exit criteria and data needed to move from cybersecurity DT&E to cybersecurity OT&E. Exit criteria should rely on data that demonstrates the PM has used an MBCRA, testing, and countermeasures to remediate any high-risk cybersecurity or resilience deficiencies discovered in cybersecurity DT&E that would prevent the system from accomplishing its operational mission(s). Mitigations not implemented before fielding do not necessarily keep a system from moving into OT. The Program Office documents cybersecurity deficiencies that remain into OT&E.

Cybersecurity DT&E should answer the following questions before moving to OT&E (note that this evaluation does not supersede Service/Component requirements):

- What are the results of the adversarial DT&E test?
  - What vulnerabilities were successfully exploited?
  - Were there mission impacts from exploited vulnerabilities; what were their severity?
  - Did mitigate and recovery capabilities perform as expected?
  - What were the test limitations?

- What are the results of the RMF security controls assessment?
  - Does the system have an ATO?
  - Are all deficiencies resolved?
  - Is there a plan and schedule for remediating critical unresolved vulnerabilities before beginning OT?
  - If mitigation or remediation efforts have been completed, have they been tested and included in the DT&E evaluation report?

- What are the recommended corrective actions?
  - For the PM?
  - For the user?
  - For the host environment, CSSP, and DCO?
7.4 Outputs

The following outputs inform oversight organization assessments, ATO decisions, and the Operational Test Readiness Review (OTRR):

- ACD event assessment reports
- Inform the RMF POA&M with test results
- A cybersecurity evaluation used to inform MS C and other acquisition program decisions
- An updated MBCRA based on Phase 4 T&E results

7.4.1 TEMP Updates

The CDT updates the TEMP for MS C and includes the plan for any remaining ACD events that will be conducted and the description of the completed events.

7.4.2 Acquisition Reviews and Decisions Informed by T&E

The system DEF describes the ACD event data that informs specific decisions. The CDT submits the cybersecurity evaluation for each ACD event to the PM. ACD events inform the following acquisition decisions:

- CDR, if an ACD event was performed early enough (recommended)
- Limited Deployment ATP
- IATT/ATO
- Milestone C
- Low Rate Initial Production
- OTRR

ACQUISITION PROGRAM RANGE EXPERIENCE: “Our ‘building-block’ approach to cyber developmental testing uses a cyber range and a ‘Build-Test-Fix-Test’ methodology. Our Program Manager stated that by using this approach, the Program Office has exhibited a positive learning curve, applying corrective actions to earlier findings and analysis from follow on test events. This was affirmed by the vulnerability assessment teams during their recent review of the test findings when comparing the findings to a previous event for the system. The Program Manager expressed an intent to continue to return to the range for additional events.”
8 Phase 5: Cooperative Vulnerability and Penetration Assessment

The purpose of testing cybersecurity during OT&E is to assess the ability of the system to enable operators to execute critical missions and tasks in the expected operational environment. The CVPA phase, required by the 2018 DOT&E Memorandum (see Section 2.5) as well as DoDI 5000.02, Enclosure 14, consists of an overt and cooperative examination of the system to identify vulnerabilities. The purpose of the CVPA phase are to provide a comprehensive characterization of the cybersecurity and resilience status of a system in a fully operational context and provide reconnaissance of the system to support adversarial testing. Figure 8-1 shows Phase 5 inputs, key tasks, and outputs. Appendix A provides a quick-look table of the tasks. Appendix F depicts a sample RASCI breakdown of the tasks.

Figure 8-1. Phase 5: Cooperative Vulnerability and Penetration Assessment Activities

8.1 Schedule

Early engagement with the OTA begins during Phase 2 to plan for the CVPA or to plan to integrate Phase 3 data from the CVI into the necessary data for the CVPA. The CVPA can be a standalone test event, a series of test events (either separate from or embedded in other tests) or an operational component of an integrated test. PMs should attempt to schedule CVPAs far enough in advance of the AA to enable mitigation of vulnerabilities before proceeding to the AA. Testing in this phase depends on the following considerations:

- **System developmental and design maturity.** The CVPA examines a mature system design in a representative operational environment and must include the intended real-world operators for the system (e.g., Soldiers, Airmen, Sailors, Marines, etc.) during CVPA. The OTA should consider the timing for delivery and availability of mature representative systems for this evaluation when developing the test schedule. If integrated with a CVI, the event must meet all data requirements for a CVPA as well as meet criteria for being production representative, independent, and operationally realistic.

- **Software/system maturity (status of previously identified shortfalls).** The CVPA begins either after previously identified CVI and ACD significant shortfalls have been resolved or with test plan documented mitigations. The test schedule must allow time to resolve the shortfalls and document mitigations, or to address the inability to resolve or document mitigations before the CVPA.

- **DOT&E or appropriate OT&E guidance.** The test strategy as documented in an approved TEMP will provide guidance that will establish expectations on the composition and specific timing of the CVPA for the system.

- **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. CVPA activities conducted before MS C require prior DOT&E approval. For a post-MS C CVPA, the operational assessment will use information from previous phases. Integrated testing is encouraged to maximize information from testing resources.
Accreditation and Authorization processes should inform OT&E, but are not substitutes for OT&E, and completion of these processes may be necessary prior to the conduct of OT&E.

### 8.2 Inputs

The following Program Office artifacts or activities are inputs to this phase:

- System’s PPP, SEP, and VOLT report
- ATO—this includes all systems and environments needed to support a continuity of operations evaluation.
- Test results from government and contractor DT&E and any integrated tests previously conducted.
- Evidence that previously identified significant shortfalls are resolved or mitigated and documented in the test plan.
- All residual DT&E is completed and an updated cybersecurity evaluation such as a DT&E assessment from DT&E or the Service/Component, in support of an OTRR, is completed.
- OTRR is completed.
- The appropriate authority (DOT&E for acquisition programs under oversight) has approved the operational test plan, including cybersecurity testing.
- The updated MBCRA based on Phase 4 T&E results.

PMMs should provide all necessary system documentation to the OTA and DOT&E (including but not limited to) system architectures, network diagrams, systems engineering plans, program protection plans, user manuals, training materials, tactics guides and procedures, certification and accreditation artifacts, results of previous testing, technical specifications, and any unique or proprietary materials.

### 8.3 Tasks

The OTA has the lead role for testing and reporting. Because this is an OT&E event, the OTA is responsible for planning, conducting, and reporting the CVPA, even if combining the CVPA with a CVI or another DT&E.

#### 8.3.1 Plan CVPA

The OTA is responsible for developing the analytical framework of issues, measures, and data requirements; the data collection procedures, including instrumentation, recording of observations and actions, and surveys; the framework of the test design, such as length, scenarios, and vignettes; and providing a report that addresses the collected data and evaluation results. CVPA data and tests include system and network scans, vulnerability validation, penetration tests, access control checks, physical inspection, personnel interviews, and reviews of system architecture and components to characterize the cybersecurity defensive status of a system as deployed and operated in the operational environment, including third party defenders.

The OTA should plan to examine operational resilience including key attributes such as:

- **Prevent:** The ability to protect critical mission functions from cyber threats.
- **Mitigate:** The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.
- **Recover:** The resilience to recover from cyber-attacks and prepare mission systems for the next fight.
The OTA should coordinate the details with the CyWG and Program Office stakeholders and document them in the operational test plan and reports. The following factors should be used to determine the scope of cyber assessments:\(^2\):

- **Operational context.** Identify the missions supported, the operators, the cyber defensive capabilities and support (including third party cybersecurity defenders and physical security), and the means by which the OTA can obtain cybersecurity defense data within those contexts.
- **System extent.** Identify risks to critical missions from the system supply chain as well as external (or “plug in”) capabilities and determine whether they should be assessed as part of the system attack surface. This may include maintenance peripherals, mission loaders, and other similar devices.
- **System-unique attributes.** Review system architectures and operating processes to identify system and network attributes that may enable attack vectors for the SUT. Identify all key performance parameters and operational requirements (such as CSEIG requirements) that require verification.
- **Specialized and system unique components.** Identify components such as cross-domain solutions, industrial controls, non-internet data transfers, and data transfer via alternate media such as radio frequency and data links.

Test planning should consider the following resources:

- Qualified team to act as the Cybersecurity Vulnerability Assessment Team (CVAT).
- Authorized tools to assess system cybersecurity (typically the cybersecurity T&E team provides).
- The SUT, including operating system and software applications and all interfacing systems needed to exercise critical data exchanges and information services, including system unique equipment.
- Representative network architecture and infrastructure, including supporting network infrastructure (routers, servers) and network defense capabilities (CSSPs, firewalls, network, and automated host-based intrusion detection devices). The intent is to create a representative cybersecurity and resilience 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).
- Results from a MBCRA, CTT, concept rehearsal, or similar analysis, available to DOT&E, the OTA, and teams supporting both the CVPA and AA
- Operational test range(s) and system/network simulations where appropriate and authorized. AA Red Team and infrastructures such as ranges and labs require scheduling well in advance. The overall T&E schedule must include AA testing events.
- Cyber ranges, if necessary, with appropriate verification, validation, and accreditation completed for OT&E—the Program Office must conduct verification and validation, and the OTA must conduct accreditation if plans include using cyber range/lab to support OT events.

The CDT documents all planning details regarding the CVPA in the MS C TEMP in accordance with OTA and/or DOT&E guidance.

### 8.3.2 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 CVAT for the event is among the most important tasks to begin early in the test planning. Coordination should include establishing a schedule,

---

\(^2\) DOT&E Memorandum, *Cybersecurity Operational Test and Evaluation Priorities and Improvements* (27 Jul 2016)
Phase 5: Cooperative Vulnerability and Penetration Assessment

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 planned as an integrated test event, then
the PM facilitates coordination among all involved test organizations and agencies to identify all data
requirements.

8.3.3 Execute CVPA and Document Results

The OTA documents all discovered vulnerabilities and provides the documentation to the Program Office,
OT&E authority, and DOT&E (as appropriate). The CVPA report should document the system
configuration as observed, all test events executed (including both failed and successful events),
observations, findings, and results. The OTA ensures the authorized tools used to assess system
cybersecurity are removed after testing is completed.

8.4 Outputs

The following are outputs from this phase to complete before entering the next phase, adversarial
assessment:

- The CVPA report documents all discovered vulnerabilities.
- The Program Office has developed a POA&M for remediating all major vulnerabilities.
- The Program Office has documented operational implications of uncorrectable vulnerabilities.
- The Program Office has updated the MBCRA based on Phase 5 T&E results.

8.4.1 TEMP Updates

- The DOT&E TEMP Guidebook (http://www.dote.osd.mil/tempguide/index.html) provides
guidance for cybersecurity content in the TEMP.

8.4.2 Acquisition Reviews and Decisions Informed by T&E

- MS C
- LRIP
- Limited Deployment and Full Deployment ATPs
9 Phase 6: Adversarial Assessment

The AA phase, required by the 2018 DOT&E Memorandum (see Section 2.5) as well as DoDI 5000.02 Enclosure 14, characterizes the operational mission effects to critical missions caused by threat-representative cyber activity and assesses the ability of a unit trained and equipped with a system to support its missions in the expected operational environment. The AA phase also assesses the effectiveness of the system’s defensive capabilities.

This phase uses an NSA-certified Red Team accredited through the USCC. In addition to assessing the effect on mission execution, the OTA shall evaluate the ability of the system, tiered defenses, and defenders to protect critical mission functions; detect and respond to cyber-attacks; and assess system resilience to survive and recover from attacks, and complete critical missions and tasks. The system encompasses all hardware, software, user operators, maintainers, training, documentation, help desk, and the TTPs used to carry out the CONOPS.

OTAs should examine relevant insider, nearsider, and outsider threat postures. More information is available in Appendix X2 discussing these threats. With prior DOT&E approval OTAs may use closed environments, cyber ranges, or other validated and operationally representative tools to demonstrate mission effects if personnel or equipment safety considerations constrain the OTA’s ability to demonstrate these mission effects.

The term “adversarial” describes only the focus of the assessment – how an adversary could exploit the system. The OTA, Program Office, user SMEs, and supporting agencies should work together in the design of the AA, use of trusted agents, and system accesses.

Figure 9-1 shows Phase 6 inputs, key tasks, and outputs. Appendix A provides a quick-look table of the tasks. Appendix F depicts a sample RASCI breakdown of the tasks.

9.1 Schedule

The OTA will conduct the AA before the Full Rate Production (FRP) or Full Deployment Decision (FDD). The AA can occur during or in support of the Initial Operational Test and Evaluation (IOT&E). The duration of the AA will depend upon the details of the system design and cybersecurity threat, but a minimum of one to two weeks of dedicated testing is a nominal planning factor, with an additional preparation period for threat reconnaissance and research activity.

9.2 Inputs

The following system artifacts or activities, as well as the specific results or report of the CVPA, serve as inputs to this phase:

- ATO
- Previous testing results that confirm that the system is capable of operation in the intended operational environment, including all interfaces, systems, and environments needed to support a continuity of operations evaluation
- Remediation of all major cybersecurity vulnerabilities identified in previous testing by verified corrections, documented user-accepted mitigation procedures, or documented acceptance of risk that the Service Acquisition Agent has submitted.
- Appropriate authority approves the TEMP and operational test plan (DOT&E for acquisition programs under oversight)
- Completed verification, validation, and accreditation for all ranges and simulations involved in the event—the Program Office must conduct verification and validation and the OTA must conduct accreditation if plans include using a cyber range/lab to support OT events.
- Operators, system administrators, and network administrator have completed training on the use and configuration of the system in an operational environment
- Most recent MBCRA results, if available

### 9.3 Tasks

The OTA has the lead role for conducting and reporting the results of the AA.

#### 9.3.1 Plan Adversarial Assessment

The OTA is responsible for developing the analytical framework of issues, measures, and data requirements; integration of CVPA results; the data collection procedures, including 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 CyWG and Program Office stakeholders and documented in the operational test plan and reports. Test planning should consider the following resources:

- Qualified and certified adversarial assessment team (NSA-certified/USCC Red Team) to act like the threat representative cyber-attack team
- Authorized tools to assess system cybersecurity and resilience (typically the cybersecurity T&E team provides)
- Production-representative and operationally configured system; any test/system deviations must be identified and approved by DOT&E prior to test. The SUT should include operating system and software applications and all interfacing systems needed to exercise critical data exchanges and information services
- Operational facilities and platforms that are representative of those expected for the deployed SUT
- Representative system architecture, including supporting network infrastructure (routers, servers), network defense capabilities (CSSPs, 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 operates).

#### Red and Blue Teams

While there are no set criteria for certifying Vulnerability Assessment Teams or Blue Teams, Red Teams must be certified by the NSA and accredited through U.S. Cyber Command to ensure they are able to transit DoD networks without doing harm to government systems. Sponsoring agencies usually qualify Blue Teams. CJCSM 6510.03 describes Red Team certification and accreditation.
Phase 6: Adversarial Assessment

- Resilience and continuity plans to include protecting backups and failovers against compromise to enable restoration to a secure state as applicable. Representative operators and cybersecurity defenders, including CSSPs.
- Operational test range(s) and system/network simulations where appropriate and authorized.
- Cyber ranges, if necessary, with appropriate verification, validation, and accreditation for the emulated system(s).

OTAs will ensure complete verification, validation, and accreditation (VV&A) of these closed environments, cyber ranges, or other validated and operationally representative tools according to Service VV&A standards.

The CDT documents all planning details regarding the AA in the MS C TEMP in accordance with OTA and/or DOT&E guidance.

9.3.2 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 window of opportunity for scheduling, 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 planned as an integrated test event, the PM should facilitate coordination among all involved test organizations and agencies to identify all data requirements. The CDT documents all planning details regarding the AA in the MS C TEMP.

9.3.3 Execute AA and Document Results

The OTA conducts the AA and provides a report that assesses the operational effectiveness, suitability, and (in some cases) survivability of the system(s) under test due to cybersecurity vulnerabilities and the resulting mission effects. DOT&E requires test reports to be provided to the AO as test results may impact the ATO. The OTA and DOT&E, when the system is under oversight, use the results to inform the operational evaluation based on test results and analysis, integrating the results of multiple measurements, which include the measurement of cybersecurity and resilience. The OTA ensures authorized tools used to assess system cybersecurity and resilience are removed after testing is completed.

9.4 Outputs

- Operational evaluation
- Program Office updates an MBCRA based on Phase 6 T&E operational evaluation
- The Program Office has developed a POA&M for remediating all major vulnerabilities

9.4.1 TEMP Updates

- The DOT&E TEMP Guidebook (http://www.dote.osd.mil/tempguide/index.html) provides guidance for cybersecurity content in the TEMP.

9.4.2 Acquisition Reviews and Decisions Informed by T&E

- Full Rate Production/Full Deployment
- Full Deployment ATP
# Acronyms and Glossary of Terms

## 10.1 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>A&amp;A</td>
<td>Assessment and Authorization</td>
</tr>
<tr>
<td>AA</td>
<td>Adversarial Assessment</td>
</tr>
<tr>
<td>ACD</td>
<td>Adversarial Cybersecurity DT&amp;E</td>
</tr>
<tr>
<td>ACDT</td>
<td>Adversarial Cybersecurity Developmental Test</td>
</tr>
<tr>
<td>AO</td>
<td>Authorizing Official</td>
</tr>
<tr>
<td>AT</td>
<td>Anti-Tamper</td>
</tr>
<tr>
<td>ATO</td>
<td>Authorization to Operate</td>
</tr>
<tr>
<td>ATP</td>
<td>Authority to Proceed</td>
</tr>
<tr>
<td>AVA</td>
<td>Architectural Vulnerability Assessment</td>
</tr>
<tr>
<td>BCAC</td>
<td>Business Capability Acquisition Cycle</td>
</tr>
<tr>
<td>C4ISR</td>
<td>Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
</tr>
<tr>
<td>CAPEC</td>
<td>Common Attack Pattern Enumeration and Classification</td>
</tr>
<tr>
<td>CDD</td>
<td>Capability Development Document</td>
</tr>
<tr>
<td>CDR</td>
<td>Critical Design Review</td>
</tr>
<tr>
<td>CDRL</td>
<td>Contract Data Requirements List</td>
</tr>
<tr>
<td>CDT</td>
<td>Chief Developmental Tester</td>
</tr>
<tr>
<td>CEVA</td>
<td>Cyber Economic Vulnerability Assessment</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Intelligence Parameter</td>
</tr>
<tr>
<td>CJCSM</td>
<td>Chairman of the Joint Chiefs of Staff Manual</td>
</tr>
<tr>
<td>COI</td>
<td>Critical Operational Issues</td>
</tr>
<tr>
<td>CONEMPS</td>
<td>Concept of Employment</td>
</tr>
<tr>
<td>CONOPS</td>
<td>Concept of Operations</td>
</tr>
<tr>
<td>COTS/GOTS</td>
<td>Commercial off-the-Shelf/Government off-the-Shelf</td>
</tr>
<tr>
<td>CPD</td>
<td>Capability Production Document</td>
</tr>
<tr>
<td>CPI</td>
<td>Critical Program Information</td>
</tr>
<tr>
<td>CRD</td>
<td>Capability Requirements Document</td>
</tr>
<tr>
<td>CSA</td>
<td>Cybersecurity Attributes</td>
</tr>
<tr>
<td>CSRC</td>
<td>Cybersecurity Risk Categorization</td>
</tr>
<tr>
<td>CSSP</td>
<td>Cybersecurity Service Provider</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>CTI</td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>CTM</td>
<td>Cyber Threat Modules</td>
</tr>
<tr>
<td>CTT</td>
<td>Cyber Table Top</td>
</tr>
<tr>
<td>CVAT</td>
<td>Cybersecurity Vulnerability Assessment Team</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>CVI</td>
<td>Cooperative Vulnerability Identification</td>
</tr>
<tr>
<td>CVPA</td>
<td>Cooperative Vulnerability and Penetration Assessment</td>
</tr>
<tr>
<td>CWE</td>
<td>Common Weakness Enumeration</td>
</tr>
<tr>
<td>CyWG</td>
<td>Cybersecurity Working Group</td>
</tr>
<tr>
<td>DAG</td>
<td>Defense Acquisition Guidebook</td>
</tr>
<tr>
<td>DASD</td>
<td>Deputy Assistant Secretary of Defense</td>
</tr>
<tr>
<td>DBS</td>
<td>Defense Business Systems</td>
</tr>
<tr>
<td>DCO</td>
<td>Defensive Cyber Operations</td>
</tr>
<tr>
<td>DEF</td>
<td>Developmental Evaluation Framework</td>
</tr>
<tr>
<td>DIA</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>DITL</td>
<td>Defense Intelligence Threat Library</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoDAF</td>
<td>DoD Architecture Framework</td>
</tr>
<tr>
<td>DoDI</td>
<td>Department of Defense Instruction</td>
</tr>
<tr>
<td>DoDIN</td>
<td>Department of Defense Information Networks</td>
</tr>
<tr>
<td>DOT&amp;E</td>
<td>Director, Operational Test and Evaluation</td>
</tr>
<tr>
<td>DRFP-RD</td>
<td>Development Request for Proposal Release Decision</td>
</tr>
<tr>
<td>DSQ</td>
<td>Decision Support Questions</td>
</tr>
<tr>
<td>DT</td>
<td>Developmental Test</td>
</tr>
<tr>
<td>DT&amp;E</td>
<td>Developmental Test and Evaluation</td>
</tr>
<tr>
<td>ECP</td>
<td>Engineering Change Proposal</td>
</tr>
<tr>
<td>EMD</td>
<td>Engineering, Manufacturing, and Development</td>
</tr>
<tr>
<td>FDD</td>
<td>Full Deployment Decision</td>
</tr>
<tr>
<td>FRP</td>
<td>Full-Rate Production</td>
</tr>
<tr>
<td>HWIL</td>
<td>Hardware-in-the-Loop</td>
</tr>
<tr>
<td>IATT</td>
<td>Interim Authority to Test</td>
</tr>
<tr>
<td>ICD</td>
<td>Initial Capabilities Document</td>
</tr>
<tr>
<td>IOT&amp;E</td>
<td>Initial Operational Test and Evaluation</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Information Support Plan</td>
</tr>
</tbody>
</table>

Acronyms and Glossary of Terms
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS ICD</td>
<td>Information Systems ICD</td>
</tr>
<tr>
<td>IS CDD</td>
<td>Information System CDD</td>
</tr>
<tr>
<td>ISSE</td>
<td>Information System Security Engineer</td>
</tr>
<tr>
<td>ISSM</td>
<td>Information System Security Manager</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>JCIDS</td>
<td>Joint Capabilities Integration and Development System</td>
</tr>
<tr>
<td>JROC</td>
<td>Joint Requirements Oversight Council</td>
</tr>
<tr>
<td>JROCM</td>
<td>Joint Requirements Oversight Council Manual</td>
</tr>
<tr>
<td>KPP</td>
<td>Key Performance Parameter</td>
</tr>
<tr>
<td>KSA</td>
<td>Key System Attribute</td>
</tr>
<tr>
<td>LRIP</td>
<td>Low Rate Initial Production</td>
</tr>
<tr>
<td>MBCRA</td>
<td>Mission-Based Cyber Risk Assessment</td>
</tr>
<tr>
<td>MDA</td>
<td>Milestone Decision Authority</td>
</tr>
<tr>
<td>MDAP</td>
<td>Major Defense Acquisition Program</td>
</tr>
<tr>
<td>MEF</td>
<td>Mission Essential Functions</td>
</tr>
<tr>
<td>MS</td>
<td>Milestone</td>
</tr>
<tr>
<td>MSA</td>
<td>Material Solution Analysis</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NVD</td>
<td>National Vulnerability Database</td>
</tr>
<tr>
<td>OEF</td>
<td>Operational Evaluation Framework</td>
</tr>
<tr>
<td>OPFOR</td>
<td>Opposing Force</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Test</td>
</tr>
<tr>
<td>OT&amp;E</td>
<td>Operational Test and Evaluation</td>
</tr>
<tr>
<td>OTA</td>
<td>Operational Test Agency</td>
</tr>
<tr>
<td>OTRR</td>
<td>Operational Test Readiness Review</td>
</tr>
<tr>
<td>OV</td>
<td>Operational View</td>
</tr>
<tr>
<td>PDR</td>
<td>Preliminary Design Review</td>
</tr>
<tr>
<td>PIT</td>
<td>Platform Information Technology</td>
</tr>
<tr>
<td>PM</td>
<td>Program Manager</td>
</tr>
<tr>
<td>PMR</td>
<td>Prevent, Mitigate, Recover</td>
</tr>
<tr>
<td>POA&amp;M</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>PPP</td>
<td>Program Protection Plan</td>
</tr>
<tr>
<td>RASCI</td>
<td>Responsible Accountable Supporting Consulted Informed</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
</tbody>
</table>

Acronyms and Glossary of Terms
### Acronyms and Glossary of Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>ROE</td>
<td>Rules of Engagement</td>
</tr>
<tr>
<td>SCA</td>
<td>Security Controls Assessor</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SE</td>
<td>Systems Engineering</td>
</tr>
<tr>
<td>SEP</td>
<td>System Engineering Plan</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Experts</td>
</tr>
<tr>
<td>SoS</td>
<td>System of Systems</td>
</tr>
<tr>
<td>SS KPP</td>
<td>System Survivability Key Performance Parameter</td>
</tr>
<tr>
<td>SSE</td>
<td>Systems Security Engineer</td>
</tr>
<tr>
<td>SSWG</td>
<td>Systems Security Working Group</td>
</tr>
<tr>
<td>STIG</td>
<td>Security Technical Implementation Guide</td>
</tr>
<tr>
<td>SUT</td>
<td>System Under Test</td>
</tr>
<tr>
<td>SV</td>
<td>Systems View</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>T&amp;E</td>
<td>Test and Evaluation</td>
</tr>
<tr>
<td>TEMP</td>
<td>Test and Evaluation Master Plan</td>
</tr>
<tr>
<td>TMRR</td>
<td>Technology Maturation and Risk Reduction</td>
</tr>
<tr>
<td>TRD</td>
<td>Technical Requirements Document</td>
</tr>
<tr>
<td>TRR</td>
<td>Test Readiness Review</td>
</tr>
<tr>
<td>TSN</td>
<td>Trusted Systems and Networks</td>
</tr>
<tr>
<td>TTPs</td>
<td>Tactics, Techniques, and Procedures</td>
</tr>
<tr>
<td>USCC</td>
<td>US Cyber Command</td>
</tr>
<tr>
<td>VOLT</td>
<td>Validated Online Lifecycle Threat</td>
</tr>
<tr>
<td>WIPT</td>
<td>Working Integrated Product Team</td>
</tr>
</tbody>
</table>

### 10.2 Cybersecurity T&E Glossary of Terms

The following are definitions of terms useful for Cybersecurity T&E.

**Anti-Tamper**

Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.

**Blue Team or Vulnerability Assessment 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 cyber-attacks 1) over a significant timeframe, 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. A Blue Team is often employed by itself or before a Red Team employment to ensure that the customer's networks are as free from flaws as possible before having the Red Team test the systems. For additional information on their application during T&E, refer to DAG, Chapter 8, T&E.

**Contract Data Requirements List (CDRL)**
A list of requirements that are authorized for a specific acquisition and made a part of the contract. It is the standard format for identifying potential data requirements in a solicitation and deliverable data requirements in a contract. The CDRL provides a contractual method to direct the contractor to prepare and deliver data that meets specific approval and acceptance criteria.

**Critical Program Information**
U.S. capability elements that contribute to the warfighters’ technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

**Critical Technical Parameters**
A measurable critical system characteristic that, when achieved, allows the attainment of a desired operational performance capability. CTPs are measures derived from desired user capabilities and are normally used in DT&E. CTP must have a direct or significant indirect correlation to key CDD and, required system specifications or CONOPS. CTPs must be focused on critical design features or risk areas.

**Cyber Tabletop Exercise**
A CTT is a low technology, low cost, intellectually intensive exercise to introduce and explore the effects of cyber offensive operations on the capability of a system, SoS, or Family of Systems to execute a mission. PMs use CTTs to identify, size and scope the cybersecurity test effort and to identify a system’s potential threat vectors, risks associated with threat vectors, potential threats from boundary systems.

**Cyber-attack**
An attack, via cyberspace, targeting an enterprise’s use of cyberspace to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure; destroy the integrity of the data; or steal 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).

**Cyber Threat Intelligence SME**
The cyber-intelligence SME is an authority on cyber-threat intelligence.
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 DT&E Technical Operators
Personnel with expertise in work related to measuring, recording, and evaluating systems along with using instrumentation, software, and test equipment to test systems.

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. See DAG Chapter 8, Section 5.3.2.

Cybersecurity Requirements
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 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 system’s overall SE process, and document this approach in the system’s Systems Engineering Plan and PPP. Working in concert with the CDT, 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.

Cybersecurity SME
The SME is a person who demonstrates an authoritative knowledge in an area or topic. The cybersecurity SME will be an authority on cybersecurity.

Cybersecurity Vulnerability Assessment Team (CVAT)
See Blue Team.

Cyber Range
An event environment that supports cyber effects on information technology; weapons; C4ISR; and other network-enabled technologies for experimentation, testing, training, or exercising on a real or simulated network. It includes hardware, software, and connectivity; test facilities; test beds; tailored scenarios; other means and resources for testing, training, and developing software; personnel; and tools. A range can be a single facility or a federation of capabilities that provides a complete, realistic mission environment for the system under test or to meet the training objectives. A range is designed to be persistent and support various events over its lifetime. For more information about Cyber Ranges, see Appendix X4.

Defense Business Systems
A developed system that reflects key aspects of capital planning and investment control best practices. The systems support efficient business processes that have been reviewed and uses an acquisition and sustainment strategy that prioritizes commercial software and products.

Derived Cybersecurity Requirements
These arise from constraints, consideration of issues implied but not explicitly stated in the requirements baseline, factors introduced by the selected architecture, cybersecurity requirements, and design. Derived

Acronyms and Glossary of Terms
requirements are definitized through requirements analysis as part of the overall systems engineering process and are part of the allocated baseline.

**Digital Twin**
A digital twin is an environment that is a digital replica of hardware, software, applications, processes and connections to interfacing systems (i.e. via a cyber range) that can be used for functional, interoperability, cybersecurity and resilience developmental testing.

**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 referred to as derived requirements) are those that can arise from technology choices, such as the use of COTS/GOTS, planned system interfaces, and protocols.

**Information System Security Manager**
Personnel responsible for the information assurance of an organization, system, or enclave.

**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 system T&E plan.

**Lead DT&E Organization**
The Lead DT&E Organization Designation Process facilitates the selection of the best suited and qualified test organization that can plan and execute DT&E activities for a project/system. The process is initiated and executed by the Program Office’s Integrated Test Team (ITT). After the process, a single Lead DT&E Organization will be nominated by the ITT and approved by the Program Executive Officer.

**Lead DT&E Organization Representative**
A representative from the Lead DT&E Organization. The Lead DT&E Organization is a government test organization and is independent from the Program Office, when feasible. The Lead DT&E Organization has responsibility for:

- Providing technical expertise on T&E issues to the CDT for the system.
- Conducting DT&E activities for the system, as directed by the CDT.

The Lead DT&E Organization assists the CDT in providing oversight of contractors under the acquisition program and in reaching technically informed, objective judgments about contractor DT&E results.

**Lead Systems Engineer Representative**
The Lead Systems Engineer is responsible for leading and implementing aspects of designing the system, from understanding the user needs, developing the business case, and working with the team to develop the technical structure of the system.
Mission-Based Cyber Risk Assessment
The process of identifying, estimating, assessing, and prioritizing risks based on impacts to DoD operational missions resulting from cyber effects on the system(s) being employed.

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 must be appropriately qualified and certified. Red Teams are certified by a board at NSA and accredited through USCC to ensure that they can 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 team of people NSA-certified and USCC-accredited 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 cybersecurity posture by demonstrating the impacts of successful cyber-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 DAG, Chapter 8, T&E.

Security Control Assessor
The Security Control Assessor is responsible for assessing the management, operational, assurance, and technical security controls implemented on an information system via security testing and evaluation (ST&E) methods.

Susceptibility
Any intentional or unintentional weakness, feature, or situation that could potentially assist an adversary in conducting a cyber-attack on a system.

Systems Security Engineer
A key discipline to protect technology, components, and information from compromise through the cost-effective application of protection measures to mitigate risks posed by threats and vulnerabilities.

Tactics, Techniques and Procedures
The TTPs are patterns of behavior used to create a standard way of operating. They can also be adversarial patterns that are used to gain actionable intelligence against an enemy style of attacking.

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 Product Team oversight representatives may participate in or observe WIPT deliberations. To be effective, the T&E WIPT should have a charter empowering it to coordinate among all the member organizations. (DAG)
**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 system’s TEMP and executed within DT&E (during the EMD phase), using a Blue Team activity to assist in the assessment. For more information, refer to DAG, Chapter 8, T&E. (NIST SP 800-39)

**Vulnerability Assessment Team**
See Blue Team.
11 References

References for Cybersecurity T&E:

- DoD Instruction 8500.01, Cybersecurity, March 14, 2014.
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.03, Department of Defense Cyber Red Team Certification and Accreditation, February 28, 2013.
- DOT&E Test and Evaluation Master Plan (TEMP) Guidebook, 19 January 2017, Version 3.1

References Risk Management Framework (RMF):

- DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014.

Other References:

- Chairman of the Joint Chiefs of Staff (CJCS) Instruction, Joint Capabilities and Development System (JCIDS), January 23, 2015.
- CJCS Manual 6510.03 DoD Cyber Red Team Certification and Accreditation, 28 February 2013.
- DoD Instruction 5000.02, Operation of the Defense Acquisition System, Enclosures 4 and 5 on DT&E and OT&E, respectively, September 14, 2017.
- DoD Instruction 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), March 17, 2016, Incorporating Change 1, July 27, 2017.
- DoD Instruction 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), May 21, 2014.
• DoD Instruction 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing, October 9, 2007.
• DoD Cyber Test and Training Ranges Executive Agent First Biennial Integrated Plan, December 2017.
• Joint Chiefs of Staff, Cyber Survivability Endorsement Implementation Guide v1.01.
• Office of the Secretary of Defense, “Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)” Version 2.0, August 2015.
• DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), DoD CIO/USD(AT&L), November 5, 2012.
• DASD(SE) and DoD CIO, “Trusted Systems and Networks (TSN) Analysis”, June 2014.
• Institute for Defense Analysis, “State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation 2016”.
• Defense Acquisition University, Incorporating Test and Evaluation into Department of Defense Acquisition Contracts. October 2011
• Vulnerability Databases:
  − CAPEC at https://capec.mitre.org/data/index.html for CAPEC List
  − CVE at https://cve.mitre.org/cve for CVE list
  − CWE at https://cwe.mitre.org/data/index.html for CWE list
  − NVD at https://nvd.nist.gov/vuln for vulnerability data
Appendix A  Cybersecurity T&E Phase 1 through 6 Quick Look

This appendix provides summary quick-look tables for the Cybersecurity T&E Phases. Detailed information for each of the phases can be found in Chapters 4 through 9.

A.1 Acquisition and Review Decisions Informed by Cybersecurity T&E

Cybersecurity T&E tasks provide test data to inform key acquisition decisions throughout a system’s development and fielding. The DEF, located in the TEMP, outlines the test data required to support acquisition decisions. Appendix E explains the cybersecurity portion of the DEF.

Table A-1 summarizes the contributions of the cybersecurity T&E process to major acquisition decisions and reviews. Each cybersecurity T&E phase also identifies the decisions commonly informed.

<table>
<thead>
<tr>
<th>Cybersecurity T&amp;E Functions</th>
<th>Decision and Review Points Influenced</th>
<th>Cybersecurity T&amp;E Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early Cybersecurity Tester Involvement Activities</td>
<td>DoDI 5000.02: Milestone A, Developmental Prototype Review</td>
<td>Phase 1</td>
</tr>
<tr>
<td></td>
<td>DoDI 5000.75: Solution Analysis Authority to Proceed (ATP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DoDI 5000.75: Functional Requirements ATP, Acquisition ATP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DoDI 5000.75: Functional Requirements ATP, Acquisition ATP</td>
<td></td>
</tr>
<tr>
<td>DT&amp;E Test Execution Activities</td>
<td>DoDI 5000.02: CDR, Milestone C, Low Rate Initial Production (LRIP)</td>
<td>Phases 3, 4</td>
</tr>
<tr>
<td></td>
<td>DoDI 5000.75: Limited Deployment ATP</td>
<td></td>
</tr>
<tr>
<td>OT&amp;E Test Execution Activities</td>
<td>DoDI 5000.02: Full Rate Production (FRP) or Full Deployment Decision (FDD)</td>
<td>Phases 5, 6</td>
</tr>
<tr>
<td></td>
<td>DoDI 5000.75: Full Deployment ATP</td>
<td></td>
</tr>
</tbody>
</table>

A.2 Summary Quick-Look Table for Phases 1 through 6

This section summarizes the inputs, outputs, and major tasks of Phases 1 through 6. Table A-2 provides the summary of the developmental test phases, Phases 1 through 4, while Table A-3 provides the summary of the operational test phases, Phases 5 and 6.
<table>
<thead>
<tr>
<th>Inputs</th>
<th>Major Tasks</th>
<th>Outputs</th>
</tr>
</thead>
</table>
| • Program Office Requirements Documentation  
• Cyber Surviability Risk Category (from CSEIG)  
• DBS System Functional Requirements  
• PPP, Cybersecurity Strategy  
• System Engineering Plan  
• DoDAF System Views  
• DBS Design specifications  
• DBS Capability Implementation Plan  
• System Requirements Documents  
• VOLT Report/STAR, Cyber Threat Modules  
• RMF Security Plan, RMF Security Assessment Plan  
• MBCRA | • Compile list of cybersecurity and resiliency requirements  
• Prepare for cybersecurity T&E Events  
  − Develop the initial DEF  
  − Identify supporting cybersecurity T&E resources  
  − Develop the initial OT evaluation framework  
  − Align RMF activities with the TEMP  
  − Plan and schedule an MBCRA  
  − Plan for cybersecurity T&E  
  − Develop cybersecurity T&E strategy | • Cybersecurity and resiliency requirements contained within the system development RFP  
• Updates to MBCRA |

<table>
<thead>
<tr>
<th>Phase 1 Understand Cybersecurity Requirements</th>
<th>Phase 2 Characterize Cyber Attack Surface</th>
<th>Phase 3 Cooperative Vulnerability Identification</th>
<th>Phase 4 Adversarial Cybersecurity DT&amp;E</th>
</tr>
</thead>
</table>
| • List of cybersecurity and resilience requirements assembled in Phase 1  
• CONOPS, CONEMP, User manuals  
• DBS Capability Implementation Plan  
• DBS Capability Support Plan  
• CSSP Support Plan  
• ISP  
• DoDAF operational views and system views  
• DBS Design Specifications  
• System Design Documents  
• System Interface Control Document  
• RMF Security Plan and Security Assessment Plan  
• Authorization boundary diagrams  
• Program Protection Plan  
• System Threat Assessment  
• System Engineering Plan  
• TEMP and MBCRA | • Identify the cyber-attack surface  
  − Examine system architecture, components, and data flows  
  − Analyze and decompose system mission  
  − Map mission dependencies  
  − Analyze the attack surface  
  − Characterize the cyber threat  
  − Examine cyber effects on the system and mission  
  − Develop cyber kill chain  
  − Perform or update MBCRA  
  • Document results and update test planning and artifacts  
  − Document results of cyber-attack surface analysis in a cyber-attack surface analysis report  
  − Prepare for Phase 3 and Phase 4 cybersecurity DT&E events  
  − Formulate test strategy | • Plan CVI Test Activities  
  − Develop cybersecurity test objectives  
  − Contractor testing  
  − Plan test events  
  − Document test plans  
  − Plan cyber test infrastructure  
  − Integrate system testing  
  • Conduct CVI events and document results  
  − Obtain reports  
  − Cybersecurity evaluation  
  − Update mission-based cyber risk assessment  
  • Prepare for Phase 4 adversarial cybersecurity DT&E event | • Update cyber threat assessment and kill chain analysis  
  • Plan adversarial DT&E  
  − Develop test objectives  
  − Define metrics  
  − Identify resources  
  − Develop rules of engagement  
  − Define process and test cases  
  − Plan integrated tests  
  − Document test plans  
  − Finalize preparation of test infrastructure  
  − Conduct TTR  
  • Conduct adversarial cybersecurity DT&E  
  − Perform ACD events  
  − Obtain reports  
  − Cybersecurity evaluation  
  − Exit criteria for cybersecurity DT&E |

<table>
<thead>
<tr>
<th>Phase 3 Cooperative Vulnerability Identification</th>
<th>Phase 4 Adversarial Cybersecurity DT&amp;E</th>
</tr>
</thead>
</table>
| • Cybersecurity portion of the DEF  
• Attack Surface Analysis Report from Phase 2  
• Test results from component level testing  
• Software Requirement Specification  
• Software Test Plan  
• DBS Capability Implementation Plan  
• DBS Capability Support Plan  
• Test Strategy for Phase 3  
• Updated TEMP  
• RMF Security Assessment Plan  
• RMF Security Plan  
• MBCRA results | • Update cyber threat assessment and kill chain analysis  
  • Plan adversarial DT&E  
  - Develop test objectives  
  - Define metrics  
  - Identify resources  
  - Develop rules of engagement  
  - Define process and test cases  
  - Plan integrated tests  
  - Document test plans  
  - Finalize preparation of test infrastructure  
  - Conduct TTR  
  • Conduct adversarial cybersecurity DT&E  
  - Perform ACD events  
  - Obtain reports  
  - Cybersecurity evaluation  
  - Exit criteria for cybersecurity DT&E |

Table A-2. Quick-Look Summary of DT&E Cybersecurity Phases 1 through 4

Cybersecurity T&E Phase 1 through 6 Quick Look
Table A-3. Quick-Look Summary of OT&E Cybersecurity Phases 5 and 6

<table>
<thead>
<tr>
<th></th>
<th>Phase 5 Cooperative Vulnerability and Penetration Assessment</th>
<th>Phase 6 Adversarial Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inputs</strong></td>
<td>• Authorization to Operate</td>
<td>• Authorization to Operate</td>
</tr>
<tr>
<td></td>
<td>• Test results from contactor DT&amp;E</td>
<td>• Test results suggestive that system is capable of operation in intended environment</td>
</tr>
<tr>
<td></td>
<td>• Identification of significant shortfalls</td>
<td>• Remediation of all major cybersecurity vulnerabilities previously identified</td>
</tr>
<tr>
<td></td>
<td>• Resolutions to identified shortfalls</td>
<td>• Approval of operational test plan by appropriate authority</td>
</tr>
<tr>
<td></td>
<td>• Completion of residual DT&amp;E</td>
<td>• Verification, validation, and accreditation for all ranges and simulations to be involved in the event</td>
</tr>
<tr>
<td></td>
<td>• Updated cybersecurity evaluation</td>
<td>• Training completion for operators, system administrators, and network administrator</td>
</tr>
<tr>
<td></td>
<td>• Operational Test Readiness Review</td>
<td>• Recent MBCRA results</td>
</tr>
<tr>
<td></td>
<td>• Approval of operational test plan by appropriate authority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Updated MBCRA</td>
<td></td>
</tr>
<tr>
<td><strong>Major Tasks</strong></td>
<td>• Plan CVPA</td>
<td>• Plan adversarial assessment</td>
</tr>
<tr>
<td></td>
<td>• Coordinate with a cybersecurity vulnerability assessment</td>
<td>• Coordinate with the OTA team</td>
</tr>
<tr>
<td></td>
<td>• Execute CVPA</td>
<td>• Execute the adversarial assessment</td>
</tr>
<tr>
<td></td>
<td>• Document results</td>
<td>• Document results</td>
</tr>
<tr>
<td><strong>Outputs</strong></td>
<td>• CVPA report with discovered vulnerabilities</td>
<td>• Operational evaluation</td>
</tr>
<tr>
<td></td>
<td>• POA&amp;M for remediating all major vulnerabilities</td>
<td>• Updated MBCRA</td>
</tr>
<tr>
<td></td>
<td>• Documented operational implications of non-correctable vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Updated MBCRA</td>
<td></td>
</tr>
</tbody>
</table>

A.3 Quick Look Tables for Phases 1 through 6

This section provides summaries of the Tasks, Inputs, Outputs, and Roles described in each phase of the guidebook. Chapters 4 through 9 provide the detailed descriptions for each of the phases. Appendix F provides an example of a Responsible, Accountable, Supporting, Consulting, Informed matrix with the roles involved to complete the phase tasks.
<table>
<thead>
<tr>
<th>Task</th>
<th>Inputs</th>
<th>Performed By</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form the Cyber Working Group (CyWG)</strong></td>
<td>• See Section 3.2</td>
<td>CDT</td>
<td>• Roster of Cyber Working Group members</td>
</tr>
</tbody>
</table>
| **Compile List of Cybersecurity Requirements** | • System documentation  
• JCIDS ICD, CDD, CPD  
• SEP  
• PPP  
• Cybersecurity Strategy  
• Information Support Plan (ISP) – from JCIDS  
• SRD  
• VOLT/STAR  
• RMF Security Plan  
• RMF Security Assessment Plan | CDT  
CyWG | • Cybersecurity and resilience requirements (stated, derived, essential)  
• Information pertinent to test conditions, environments, methods, or prioritization of testing  
• Testable, measurable, and achievable requirements  
• Assessment of testability, measurability, and achievability of cyber requirements in the CDD  
• Inputs to MS B RFP detailing cybersecurity T&E that the contractor will complete  
• Preliminary DT&E analysis in support of the PDR |
| **Develop the initial DEF** | • Cybersecurity capabilities that will inform DSQs  
• DAG Chapter 8 | Requirements communities  
T&E WIPT  
PM  
Chief Engineer | Evaluation issues for cybersecurity included in the TEMP’s DEF  
Identification of relevant system issues |
| **Identify cyber T&E resources** | • Threat information  
• Svc/component cyber test resources | CDT  
CyWG | Specific resources that will support cybersecurity T&E activities  
Threat portrayal to be used against the system during testing |
| **Develop the initial OT evaluation framework** | • DOT&E Memorandum 1 Aug, 2014  
• DAG, Chapter 9 | OTA  
Requirements communities | Cybersecurity measures for operational test plans within the TEMP |
| **Align RMF activities with the TEMP** | • RMF schedule and milestones | CDT  
Security Controls Assessor | Aligned RMF Security Assessment Plan with TEMP delivery  
Schedule of, and resources necessary for, controls assessment, within TEMP |
| **Plan and schedule an MBCRA** | • See Appendix X3 | CDT | See Appendix X3 |
| **Develop cybersecurity T&E strategy** | • Cybersecurity requirements that must be tested | CyWG | • Cyber T&E strategy documented in the TEMP  
• Planned cybersecurity test activities |
### Table A-5. Phase 2 – Characterize the Cyber Attack Surface Quick Look

<table>
<thead>
<tr>
<th>Task</th>
<th>Inputs</th>
<th>Performed By</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine system architecture</td>
<td>• Cybersecurity requirements from Phase 1</td>
<td>• CDT</td>
<td>• List of interfacing systems and data connections</td>
</tr>
<tr>
<td></td>
<td>• System Design Documents</td>
<td>• CyWG</td>
<td>• Points of entry/exit into the system</td>
</tr>
<tr>
<td></td>
<td>• SEP and PPP</td>
<td></td>
<td>• List of host environment provisions for protection</td>
</tr>
<tr>
<td></td>
<td>• RMF Security Plan and Security Assessment Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Criticality Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mission-essential functions and dependencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CONOPS</td>
<td>• CyWG</td>
<td>• Updated attack surface listing with potential for insider attack surface points</td>
</tr>
<tr>
<td></td>
<td>• CSSP support plan</td>
<td></td>
<td>• Identification of all human interaction with hardware, software, and firmware</td>
</tr>
<tr>
<td></td>
<td>• Roles and responsibilities of system operators and admins</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Points of entry/exit into the system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• List of host environment provisions for protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Points of entry/exit into the system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• List of host environment provisions for protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Criticality overlay applied to interfacing systems list</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service Cyber Threat Intel (CTI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Publicly available CTI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Map mission dependencies on system</td>
<td>• PPP criticality analysis</td>
<td>• CDT</td>
<td>• Map of mission dependencies on system components</td>
</tr>
<tr>
<td>components</td>
<td>• CONOPS</td>
<td>• CyWG</td>
<td>• Criticality overlay applied to interfacing systems list</td>
</tr>
<tr>
<td></td>
<td>• Criticality overlay applied to interfacing systems list</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Svc/component Intelligence organizations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Characterize the cyber threat</td>
<td>• VOLT report / STAR</td>
<td></td>
<td>• Determination of adversary motivation and capability</td>
</tr>
<tr>
<td></td>
<td>• Threat profile</td>
<td></td>
<td>• Threat profile</td>
</tr>
<tr>
<td></td>
<td>• Identified attack paths</td>
<td></td>
<td>• Identified attack paths</td>
</tr>
<tr>
<td>Examine cyber effects on the system and</td>
<td>• Adversarial TTPs</td>
<td>• CDT</td>
<td>• Determination of attack paths with mission impact</td>
</tr>
<tr>
<td>mission</td>
<td>• Cyber-attack surface</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Phase 1 results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compose cyber kill chain</td>
<td>• Range of cyber attacker activities</td>
<td>• CDT</td>
<td>• Potential attack sequences</td>
</tr>
<tr>
<td>Update MBCRA</td>
<td>• MBCRA method</td>
<td>• CyWG</td>
<td>• Evaluation of mission risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Likelihood of identified exploitation techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Prioritized list of attack surface areas</td>
</tr>
<tr>
<td>Prepare cyber-attack</td>
<td>• Prioritized attack surface list</td>
<td>• CDT</td>
<td>• Documented findings from previous tasks</td>
</tr>
<tr>
<td>surface analysis report</td>
<td>• Recommended activities</td>
<td>• CyWG</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formulate test strategy</td>
<td>• Areas of concern</td>
<td>• CDT</td>
<td>• Planned series of Phase 3 and 4 activities</td>
</tr>
<tr>
<td></td>
<td>• Acquisition Program decisions as identified in the DEF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table A-6. Phase 3 – Cooperative Vulnerability Identification Quick Look

<table>
<thead>
<tr>
<th>Task</th>
<th>Inputs</th>
<th>Performed By</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop cybersecurity test objectives</td>
<td>• Critical technical parameters</td>
<td>• CDT</td>
<td>• Cybersecurity test objectives&lt;br&gt;• Desired outcomes from test activities&lt;br&gt;• Metrics capable of demonstrating improvements in SUT development</td>
</tr>
<tr>
<td>Examine contractor T&amp;E activities</td>
<td>• Vendor contracts&lt;br&gt;• Contractor test data&lt;br&gt;• CTPs</td>
<td>• CyWG</td>
<td>• Verification that system meets stated capabilities</td>
</tr>
<tr>
<td>Plan test events</td>
<td>• Test objectives&lt;br&gt;• Required data&lt;br&gt;• Functions critical to mission success&lt;br&gt;• Vulnerability test activities</td>
<td>• CDT</td>
<td>• Prioritized cyber test activities&lt;br&gt;• Updated test objectives&lt;br&gt;• Test limitations&lt;br&gt;• Test schedule&lt;br&gt;• Required resources</td>
</tr>
<tr>
<td>Document test plans</td>
<td>• Test resources&lt;br&gt;• Test objectives&lt;br&gt;• Test schedules</td>
<td>• CDT</td>
<td>• Detailed test plans</td>
</tr>
<tr>
<td>Plan cyber test infrastructure</td>
<td>• Planned cyber test activities&lt;br&gt;• Cyber capabilities&lt;br&gt;• Performance capabilities</td>
<td>• CDT</td>
<td>• Reserved necessary test infrastructure&lt;br&gt;• Identification of safe simulation and experimental environments&lt;br&gt;• Allocated resources for disposable test articles</td>
</tr>
<tr>
<td>Integrate system testing</td>
<td>• System mission testing&lt;br&gt;• System functional testing</td>
<td>• CDT</td>
<td>• Resourced test articles&lt;br&gt;• Baseline of system performance&lt;br&gt;• Updated test plans</td>
</tr>
<tr>
<td>Conduct CVI Events</td>
<td>• Planned government test activities&lt;br&gt;• Planned contractor test activities</td>
<td>• CyWG</td>
<td>• Test data and reports</td>
</tr>
<tr>
<td>Obtain reports</td>
<td>• Test data and test results from test activities</td>
<td>• CDT</td>
<td>• Verification of implementation of mitigations and deficiency corrections&lt;br&gt;• Documentation of discovered vulnerabilities&lt;br&gt;• Recommended corrective actions</td>
</tr>
<tr>
<td>Cybersecurity evaluation</td>
<td>• See Section 3.8.1</td>
<td>• CDT</td>
<td>• See Section 3.8.1</td>
</tr>
<tr>
<td>Update MBCRA</td>
<td>• CVI test results&lt;br&gt;• Contractor T&amp;E data</td>
<td>• CyWG</td>
<td>• Updated cyber risk assessment&lt;br&gt;• Understanding of suspected mission impacts</td>
</tr>
<tr>
<td>Prepare for adversarial cybersecurity DT&amp;E</td>
<td>• Unremediated vulnerabilities&lt;br&gt;• Adversary TTPs&lt;br&gt;• Cybersecurity requirements</td>
<td>• CDT</td>
<td>• Test opportunities for SoS context testing during adversarial cybersecurity DT&amp;E</td>
</tr>
<tr>
<td>Task</td>
<td>Inputs</td>
<td>Performed By</td>
<td>Outputs</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>--------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Update cyber threat assessment and kill chain analysis | • Cyber threat assessment  
• Attack surface analysis  
• Kill chain analysis | • CDT  
• ACD test team | • Threat vignettes  
• Updated inputs with anticipated threat tactics |
| Develop test objectives | • Mission objectives  
• Adversary TTPs  
• Operating environment | • CDT  
• DCO team | • Test objectives that support evaluation of the system’s resiliency in a mission context |
| Define metrics | • Test objectives | • CDT | • Data to be collected during ACD event |
| Identify resources | • Personnel  
• System  
• Environment | • CDT | • List of required resources |
| Develop rules of engagement | • Available resources  
• PM needs  
• Legal procedures | • PM  
• ACD test team | • Rules of engagement documented in the test plan |
| Define process and test cases | • Test-fix-retest methodology | • CDT | • System configuration settings  
• Updated test goals |
| Plan integrated tests | • Test objectives | • CDT | • List of test objectives able to be combined |
| Document test plans | • Test objectives  
• Required data  
• Systems, personnel, and environment | • CDT  
• ACD test team | • Test Plans |
| Finalize preparation of test infrastructure | • Verified requirements  
• Rules of engagement | • CDT  
• OTA  
• ACD test team  
• Range event designers | • Reservation of ACD test infrastructure  
• Assessment of availability of emulated DoDIN |
| Conduct test readiness review | • Test objectives  
• Test methods | • CDT | • Test Readiness Review |
| Perform ACD events | • Threat documents  
• Threat methodology | • ACD test team | • Exposed vulnerabilities  
• Evaluation report |
| Obtain reports | • ACD test findings requiring corrective actions | • CDT | • Updated RMF POAM  
• ACD reports provided to OTA and oversight organizations |
| Cybersecurity evaluation | • ACD report  
• Cybersecurity mission impact assessment | • CDT | • Evaluation of actual and estimated mission impacts  
• Updated MBCRA |
| Exit criteria for cybersecurity DT&E | • Developmental test findings | • DT&E testers  
• OT&E testers | • Jointly established exit criteria and data to move from DT to OT |
**Table A-8. Phase 5 – Cooperative Vulnerability and Penetration Assessment Quick Look**

<table>
<thead>
<tr>
<th>Task</th>
<th>Inputs</th>
<th>Performed By</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan CVPA</td>
<td>• Qualified teams</td>
<td>• OTA</td>
<td>• Framework of issues</td>
</tr>
<tr>
<td></td>
<td>• Authorized tools</td>
<td>• CTEWG</td>
<td>• Data requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data collection procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Documented details in operational test</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>plan and reports</td>
</tr>
<tr>
<td>Coordinate with a</td>
<td>• Qualified teams</td>
<td>• OTA</td>
<td>• List of required resources</td>
</tr>
<tr>
<td>Cybersecurity Vulnerability</td>
<td></td>
<td>• PM</td>
<td>• Scheduled cybersecurity vulnerability</td>
</tr>
<tr>
<td>Assessment Team</td>
<td></td>
<td></td>
<td>assessment team</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Established schedule</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Anticipated products</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Formal report of activities and findings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data requirements</td>
</tr>
<tr>
<td>Execute CVPA and</td>
<td></td>
<td>• OTA</td>
<td>• Documented discovered vulnerabilities</td>
</tr>
<tr>
<td>document results</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table A-9. Phase 6 – Adversarial Assessment Quick Look**

<table>
<thead>
<tr>
<th>Task</th>
<th>Inputs</th>
<th>Performed By</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan adversarial assessment</td>
<td>• CVPA results</td>
<td>• OTA</td>
<td>• Test data requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CTEWG</td>
<td>• Data collection procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CDT</td>
<td>• Test scenarios</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Formal report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Documented details in operational test</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>plan and reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Documented planning details in MS C TEMP</td>
</tr>
<tr>
<td>Coordinate with the OTA</td>
<td>• PM</td>
<td>• OTA</td>
<td>• Required resources identified</td>
</tr>
<tr>
<td>team</td>
<td></td>
<td>• CDT</td>
<td>• Scheduled event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data requirements identified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Document planning details in the MS C TEMP</td>
</tr>
<tr>
<td>Execute AA and document</td>
<td></td>
<td>• OTA</td>
<td>• Assessment of operational</td>
</tr>
<tr>
<td>results</td>
<td></td>
<td></td>
<td>effectiveness, suitability, and survivability of the system</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B  Incorporating Cybersecurity T&E into DoD Acquisition Contracts

This appendix assists the DoD and industry T&E professionals in identifying T&E cybersecurity related items that may be included in a Statement of Work (SOW/Statement of Objectives (SOO), Performance Work Statement, and other sections of an RFP. For a complete understanding of incorporating T&E into DoD Acquisition Contracts, refer to the Incorporating T&E into DoD Acquisition Guide3. This appendix presumes the reader has a basic understanding of T&E and the DoD systems acquisition processes.

This appendix focuses on T&E cybersecurity related items common across DoD Components. Components may have specific T&E direction and guidance that each deems necessary for tailoring its acquisition programs.

B.1 Background

The RFP, which includes the SOW/ SOO/ PWS, is a critical contractual document that forms the basis for all initiatives that follows in the acquisition life cycle, whether the RFPs are for prototyping contracts or development contracts in the EMD phase. Addressing cybersecurity testing in these RFPs early in the acquisition life cycle allows security features to be designed into the system and decreases the possibility of significant, disruptive changes later in system development. The T&E guidance is based on systems that implement an acquisition strategy in which the development and testing have a single prime contractor. This is one of many DoD contracting strategies. Some project/system acquisitions have different contracts. The PM may tailor the T&E guidance to fit their unique situation or approach, in the context of the contract. This guidance is based on the sequenced development process of the RFP that leads to a contract.

The T&E strategy is an event-driven T&E approach linking key decisions in the system life cycle to knowledge from developmental and operational evaluations and outlines the test methodologies to obtain the data for evaluation. The T&E approach identifies specific T&E techniques that contribute to maturing the capability through discovery of deficiencies and understanding of performance levels. The T&E strategy is captured in the approved TEMP and updated at each milestone focusing on those T&E events and activities expected in the subsequent acquisition phase. The TEMP, and the included T&E strategy, include as much information known at the time of development. The TEMP is a Government document required prior to each milestone, and depending on the acquisition strategy, may be a contractual compliance document for inclusion in the RFP.

The primary theme to remember is that if a T&E item or requirement addressing cybersecurity is not in the SOW, it probably will not be in the RFP, and if it is not in the RFP, it probably will not be in the contract. If it is not in the contract, do not expect to get it!

The contractor plans and executes most of the testing that transitions technology into functional capabilities that the military requires. The contractor also plans and performs qualification testing of subcomponent parts and products from vendors that make up the system delivered to the military. Government testers need to understand the contractor testing processes, methods, and infrastructure to assess the amount of visibility needed into proposed test activities. Government testers should identify when data collection and transfer will benefit Government test activities to reduce redundant or unnecessary testing.

3 Defense Acquisition University, Incorporating Test and Evaluation into Department of Defense Acquisition Contracts (October 2011).
Experienced testers should determine cost/benefit ratios for requiring visibility into contractor proprietary activity and data transfer to the Government.

**B.2 Recommendations for DoD Request for Proposals**

A RFP is a solicitation used in negotiated acquisition to communicate government requirements to prospective contractors and to solicit proposals. At a minimum, solicitations shall describe the Government’s requirement (includes Section C), anticipated terms and conditions that will apply to the contract, information required in the offeror’s proposal (Section L), and (for competitive acquisitions) the criteria that will be used to evaluate the proposal and their relative importance (Section M). The following focuses on providing example SOW language (Section C) as well as information that can be required and evaluated from the offeror.

**B.2.1 Section C**

Section C of the RFP contains the detailed description of the products to be delivered or the work to be performed under the contract. This section typically includes the Government’s SOW (or SOO) and preliminary System Performance Specification.

The following are examples that can be used/modified for the SOW.

- Participate in the Government-led T&E WIPT and cybersecurity subgroups that support the planning, execution, analysis of data, and reporting of test results.
- Participate in mission-based cyber risk assessments (e.g., CTT exercise, etc.) to categorize potential vulnerabilities (based on capability of threat and the critical functions/components) that should be tested or analyzed.
- Provide a system-level architecture, views, and use cases (i.e., DoDAF views required by JCIDS Manual) and identify potential vulnerabilities. Update on a recurring basis.
- Provide detailed design and architecture documentation to support test planning activities.
- Identify and document testing methodologies to be implemented, including code evaluations, functional testing, penetration testing, fuzz testing, vulnerability scans, third-party assessment, and off-nominal test cases.
- Develop and test software abuse cases, network resiliency abuse cases (e.g. Denial of Service attacks), and other system misuse and abuse cases.
- Conduct cybersecurity test and evaluation on components and subcomponents as described in the TEMP.
- Expose systems and networks to realistic cyber threats in a closed test facility, by independent cyber professionals, using the latest tools, techniques, and malware to evaluate the system design.
- Conduct passive port and connection reconnaissance and if applicable active reconnaissance (web app scan, port scan, and vulnerability scan).
- Conduct network scans by running port scanners and vulnerability scanners to assess for susceptibility to known exploits.
- For mission critical components, apply manual and automated software vulnerability detection methods and automated internal code level tools (static and dynamic), application penetration and fuzz/robustness testing, and database scanning tools.
- Conduct cybersecurity testing as part of non-cybersecurity system of systems events (such as JITC interoperability testing) and integrate applicable RMF security controls assessment activities into unit testing, functional testing, etc.
- Develop and deliver Contractor Detailed Test Plans for contractor test events
- Analyze and evaluate test results in a Test and Evaluation Report for each test event.
• Track contractor identified vulnerabilities and corrective action/mitigation plans.
• Provide government access to data from contractor cybersecurity test events.
• Provide support, source data, and analysis required to support the Government in obtaining authorization for the system (IATT and ATO) in accordance with DoD Instruction 8500.01, Cybersecurity, (14 Mar 2014) and 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) (12 Mar 2014).
• Provide a digital twin of the system, System Integration Lab or Hardware in-the-Loop facility for testing. A digital twin is an environment that is a digital replica of hardware, software, applications, processes and connections to interfacing systems (i.e. via a cyber range) that can be used for functional, interoperability, cybersecurity and resilience developmental testing.

B.2.2 Section L

Section L of the RFP describes in detail the contents of each volume of the proposal. Inserted within this section of the solicitation are provisions and other information and instructions not required elsewhere to guide the offerors or respondents in preparing proposals or responses to RFPs. Prospective offerors or respondents may be instructed to submit proposals or information in a specific format or several parts to facilitate the evaluation. The instructions may specify further organization of proposal or response parts, such as administrative, management, technical, past performance, and certified cost of pricing data.

A successful offeror’s proposal must respond to the requirements of the RFP. The proposal must be responsive to and consistent with Section L, Instructions, Conditions and Notices to Offerors or Respondents. Section M will describe the standard against which the proposal will be evaluated and forms the basis for selection.

Examples for Section L:
• The offeror shall describe their overall plan and methodology for how the cybersecurity requirements will be managed, tested, evaluated and flowed down to subsystems and components including those that subcontractors/development partners have developed (as well as applied to COTS and non-developmental components)
• The offeror shall describe their overall plan for how they will develop and execute their cybersecurity vulnerability analysis and adversary threat analysis and how the results of these analyses can improve test and evaluation outcomes.
• The offeror shall describe their approach to cybersecurity risk management, including threat analysis, system exposure to threats, as well as integration of cybersecurity with systems engineering and risk management processes.
• The offeror shall describe how their approach satisfies the requirements of DISA STIGs and minimizes the overall Common Weakness Scoring System (CWSS) and Common Vulnerability Scoring System (CVSS) scores of the enterprise or standalone systems into which the software will be installed.
• The offeror shall describe how their process align with the activities described in the Cybersecurity T&E Guidebook (v2.0).
• The offeror shall describe their process to ensure all selected security controls and the cybersecurity capabilities derived from the security controls are tested and evaluated to the Authorizing Official's accepted risk level to receive an IATT and ATO for the system as required.
• The offeror shall describe their process for performing penetration testing and cyber threat-based testing based on the expected threat environment as described in the SOW.

Incorporating Cybersecurity T&E into DoD Acquisition Contracts
B.2.3 Section M

Section M, “Evaluation Factors for Award,” forms the basis for evaluating offerors' proposals and is the only section of the solicitation that communicates to offerors the criteria the Government will use to make the best value award decision. The instructions included in Section L are designed to provide guidance to the Offeror concerning documentation that will be evaluated. Section L Instructions to Offerors should be drafted concurrently with Section M factors and sub-factors. This will ensure that the offeror is providing the information needed to evaluate. Each offeror’s technical and management proposals shall be evaluated based on specific sub factors to determine if the offeror provides a sound, compliant approach that meets the requirements of the RFP and demonstrates a thorough knowledge and understanding of those requirements and their associated risks.

Example of Section L and Section M:

Section L: The offeror shall describe their overall plan and methodology for how the cybersecurity requirements will be managed, tested, evaluated and flowed down to subsystems and components including those that subcontractors/development partners have developed (as well as applied to COTS and non-developmental components).

Section M: The Government will evaluate the proposed plan and methodology for managing, testing, and evaluating cybersecurity requirements on the soundness of the contractor’s proposed approach to ensuring the comprehensive design is fully tested and meets cybersecurity requirements, and the technical understanding of cybersecurity T&E concepts is fully understood.
Appendix C  Considerations for Tailoring the Cybersecurity T&E Phases

The cybersecurity T&E process assumes cybersecurity T&E activities start shortly after acquisition program initiation and closely align with the DoDI 5000.02 full acquisition life cycle. This ideal case allows sufficient time for planning cybersecurity test activities with contractor and government engineers and cybersecurity test teams. However, acquisition programs come in many sizes with distinct timelines that do not always align with the full acquisition life cycle. For these cases, the cybersecurity T&E process is tailorable to meet unique acquisition program needs and still ensure efficiency and effectiveness of cybersecurity T&E activities.

This appendix advocates tailoring and integrating, not skipping, the phases. Early and proper execution of Phases 1 and 2 put in place the necessary means to identify and correct cybersecurity issues early in the system life cycle. Early discovery of system vulnerabilities facilitates remediation and reduces risk to acquisition program cost, schedule, and performance. Late testing renders system remediation much more difficult due to the pressures of time and lack of funding before fielding or deployment.

Tailoring the cybersecurity T&E phases is discouraged under the following conditions:

- New architecture (numerous new interfaces)
- Significant addition of key terrain items to a system architecture or system (typically when adding a new capability/large upgrades)
- Significant change in intended operational environment
- Significant changes in supply chain

Before using the guidance in this appendix, PMs should conduct an MBCRA to determine timing and scope of cybersecurity T&E phase activity. A risk-based assessment is the preferred method to tailoring cybersecurity T&E activities and provides the rationale for the subsequent cybersecurity T&E activities. CDTs and OTAs must understand the cybersecurity risks associated with what testing can and cannot be accomplished in each tailoring scenario. CDTs and OTAs must document the testing plan and associated risks in the TEMP.

Readers are strongly encouraged to be familiar with the cybersecurity T&E phases described in the main body of the guidebook before reading and applying Appendix C guidance.

C.1 General Tailoring Considerations

In planning for tailoring, CDTs continue to follow the general principle that cyber testing should occur as early as possible and during system development. Below is a summary of the key activities in the cybersecurity T&E phase process that CDTs must describe and include in their T&E documentation (TEMP, T&E strategy, implementation plan, etc.) regardless of the tailoring approach:

- **Requirements and Attack Surface Analysis** – This activity includes reviewing cybersecurity requirements and analyzing attack surfaces for critical mission systems. Phases 1 and 2 are key planning steps that help testers determine the scope of cybersecurity testing and outlines the people, tools, and infrastructure needed for subsequent phases. Conducting and repeating these phases will ensure efficient, cost effective, and adequate cybersecurity T&E.

- **Vulnerability Assessments** – Cybersecurity testers perform vulnerability assessments that are a combination of paper analysis and hardware and software testing. Phases 3 and 5 both emphasize finding and fixing vulnerabilities, and retesting systems to verify fixes. Vulnerability assessments also include exploiting vulnerabilities in the system to inform mission impact and risk assessments as well as to identify mitigations, countermeasures or other fixes if needed. Each
assessment is a snapshot in time and therefore vulnerability assessments conducted earlier and varying in scope and emphasis are more cost effective and supportive of reducing technical risk than waiting until OT&E.

- **Threat-Based Testing** – Adversarial test teams conduct penetration testing and exploitation testing of known vulnerabilities from the standpoint of a cyber adversary (Phases 4 and 6). Threat-based testing provides verification of applicable cybersecurity and resiliency requirements, and helps determine the risk and feasibility of attack vectors. Both DT&E and OT&E threat-based testing is strongly preferred.

The sections below provide tailoring considerations for time sensitive systems, urgent needs systems, software intensive (including agile development) systems, and small systems. The sections below also include tailoring considerations for cloud computing platforms and defense business systems that fall under DoDI 5000.75. Since a single system may align to multiple sections below, CDTs and OTAs may selectively tailor the approaches to optimize the three key activities. The approaches discuss MBCRA (e.g., CTT exercises) and other tools that may help PMs gain efficiencies during cyber test planning and execution.

### C.2 Time Sensitive Programs – Analysis Time Is Compressed

Systems with short acquisition timelines and compressed schedules require condensed timeframes for completing cybersecurity T&E analysis tasks (Phases 1 and 2). Important analysis steps, such as thoroughly understanding cybersecurity requirements and characterizing the attack surface, may be constrained. This scenario also occurs when initiating cybersecurity T&E planning after MS B or after contract award.

**Requirements and Attack Surface Analysis** – The most effective method to successfully save schedule and cost in cybersecurity T&E is executing Phases 1 and 2 in parallel prior to TEMP approval, since neither phase involves testing. Omitting Phases 1 and 2 analyses introduces risk to test planning and obscures test direction. Table C-1 below describes this risk.

**Vulnerability Assessments** – Conduct Phases 3 and 5 per the guidance described in the main body of this guidebook. The purpose for Phase 3 testing activities is to inform ATO and MS C decisions. Phase 3 is not just RMF controls and STIG assessments but a series of cybersecurity test events that help identify vulnerabilities that can be mitigated before final implementation. The purpose of Phase 5 is to prepare for IOT&E and inform LRIP decisions. In compressed testing timelines, CDTs may choose to integrate Phases 3 and 5 into other phases as described in Section C.3 below.

**Threat-Based Testing** – This appendix does not recommend integrating Phases 4 and 6 into a single test activity in this tailoring scenario because this results in threat based cybersecurity testing occurring only during OT&E and eliminates early discovery of mission-impacting vulnerabilities that inform MS C, OTRR, and the ATO. Eliminating Phase 4 or integrating Phases 4 and 6 constrains mitigation efforts. If Phases 1 and 2 are compressed, Phase 4 testing should allow time to expose many of the exploitable vulnerabilities not identified during the Phase 2 attack surface analysis and also allow time for adequate mitigation.
Table C-1. Compressed Cybersecurity Analysis Risks

<table>
<thead>
<tr>
<th>Delayed Tasks</th>
<th>Delayed Timeframe Issue</th>
<th>Risk</th>
<th>Risk Reduction Considerations</th>
</tr>
</thead>
</table>
| Phase 1 Understand Cybersecurity Requirements | Reduction in analysis and enumeration of implied and essential cybersecurity requirements | • Lack of analysis time results in inadequately identified or understood implied and essential requirements and poor test planning  
• DT&E and OT&E cybersecurity expertise may not be available with short notice to provide insight | • Reuse and rely on system and RMF artifacts developed for previous system increments  
• Involve Cybersecurity SMEs and Mission SMEs to perform CTT exercise  
• SUT and SoS artifacts may be more mature and useful later in the process when more is known about the prospective system design |
| Phase 2 Attack Surface Characterization    | Reduction in analysis and enumeration of system components/attack surface and vulnerabilities | • Lack of analysis time results in inaccurate enumeration of attack surface  
• More common vulnerabilities may be discovered during Phase 6 instead of earlier in DT&E, hampering the thoroughness of Phase 6 later in OT&E  
• Remediation and verification testing may not be completed prior to fielding or deployment | • Contractor designs at CDR may reveal more accurate attack surface later in Acquisition Life Cycle  
• Reuse and rely on system and RMF artifacts developed for previous system increments  
• Involve Cybersecurity SMEs and Mission SMEs to perform CTT exercise  
• Review vulnerability test results from previous increments to ensure defects were resolved |

C.3 Urgent Need Systems – Test Time Is Compressed

Urgent needs systems, including Joint Urgent Operational Needs may decide to integrate cybersecurity DT&E and OT&E. This most commonly occurs when planned cybersecurity T&E is closer to fielding or deploying the capability. Section C.4 describes the tailoring approach for incrementally deployed software intensive systems. Use of integrated cybersecurity DT&E and OT&E may be necessary when:

- A system has quickly progressed to the testing stage and must expedite fielding or deployment. Non-developmental items may fit in this category.
- A system is already past MS C when operational changes or cybersecurity shortfalls cause testing to be revisited with little or no change in fielding or deployment schedule requirements.

Compressed test timeframes may result in fielding or deploying vulnerable systems, putting warfighters at risk during mission operations due to incomplete vulnerability testing and insufficient remediation/mitigation prior to AA. This is due to discovering system vulnerabilities late in the life cycle when funding to fix vulnerabilities is not available and an urgency to deploy or field the system exists. Systems with critical vulnerabilities and no time to fix may result in a disapproved, revoked, or a conditional ATO.

When compressed test timeframes are anticipated, PMs may need to rely heavily on selecting a contractor with very mature software and hardware cybersecurity testing processes. The RFP should describe a strong role for contractor T&E including items such as contractor cybersecurity T&E data that is provided to government, and government observation of contractor cybersecurity T&E.

Requirements and Attack Surface Analysis – To use test time more effectively, the CDT should perform Phases 1 and 2 to help focus and prioritize test activities. Omitting Phase 1 and 2 analysis reduces understanding risk to test planning and results in missed opportunities for testing that could be discovered during Phase 1 and 2 analyses to addresses highest risk items. Conducting Phases 1 and 2
analyses in parallel and an MBCRA all prior to TEMP approval will provide the PM with the greatest insight for test planning.

**Vulnerability Assessment** – Since the system may be close to or post MS C, Phases 3 and 5 are integrated to inform MS C and/or ATO and production/deployment decisions. The integrated testing also informs LRIP and TRRs for adversarial assessments. Plan and schedule integrated testing for CVI and CVPA with the Lead DT&E Organization, OTA, and vulnerability analysts for DT&E to use the same schedule, lab/range, tools, and people. Evaluate data from any available contractor testing or RMF assessments during Phase 3. Table C-2 summarizes this approach.

**Threat-Based Testing** – Phases 4 and 6 are integrated. The ACD and OT&E AA is performed once using the same operational environment or simulated operational environment and at the same time with the same people and tools. Integrated testing creates opportunities for staff and facility sharing and may reduce costs. DT&E AA may benefit from test results using an NSA-certified Red Team during OT&E AA.

### Table C-2. Integrated Cybersecurity DT&E/OT&E

<table>
<thead>
<tr>
<th>DT&amp;E Cybersecurity</th>
<th>Combined with OT&amp;E Cybersecurity</th>
<th>How Does This Work?</th>
<th>Risk</th>
</tr>
</thead>
</table>
| Phase 3 CVI        | Phase 5 CVPA                     | Vulnerability Test Team performs single vulnerability assessment in a lab environment using a test, analyze, fix, and verify process followed by cooperative penetration testing and/or, reuse of RMF test data | • Lack of comprehensive SUT cybersecurity status characterization in a fully operational context  
• Less time to identify vulnerabilities  
• Insufficient time allotted to fixing discovered vulnerabilities prior to AA |
| Phase 4 ACD        | Phase 6 AA                       | Single adversarial test by NSA-certified Red Team in a mission context in a cyber-contested operational environment. | • Limitations due to operational considerations may impact the scope and effectiveness of the AA  
• More discoveries of common vulnerabilities during AA and impact threat assessment.  
• Remediation and verification testing may not be possible in the operational environment prior to fielding or deployment. |

The CDT must consider whether integrating DT&E and OT&E will prevent meeting cybersecurity T&E objectives. Some portions of DT&E and OT&E may always require separate assessments due to requirements for an independent operational assessment in an operational environment. Integrated threat-based testing may result in less comprehensive assessment of test objectives for DT&E and OT&E. The CyWG should negotiate the trade-offs needed to develop operational scenarios that work for a combined DT&E/OT&E assessment.

As an alternative and with approval from DOT&E, Phase 5 assessment requirements may be satisfied through comprehensive Phase 3 and Phase 4. Guided by an MBCRA, testers may focus only on high-risk exploitable vulnerabilities on key cyber terrain, then test for vulnerabilities in other components after fielding or deployment.
C.4 Software Intensive Programs

Software intensive systems, as described in DoDI 5000.02, Model 2, typically include several complex software builds that deliver multiple features to the end user during each software increment. These systems include planned software builds; the software builds comprise a series of testable, integrated subsets of the overall capability, which together with clearly defined decision criteria ensure adequate progress before fully committing to subsequent builds.

Software intensive systems frequently incorporate COTS and/or GOTS technology acquired and/or adopted for DoD applications. Overall system requirements usually do not change, and multiple delivery increments fulfill the entire system requirements specified. Figure C-1 illustrates this model, referred to as the Waterfall Release Cycle.

![Waterfall Release Cycle](image)

Figure C-1. Waterfall Release Cycle

Software intensive systems should ensure the contract has well defined contractor software assurance and security testing requirements for each software delivery build. Testers should verify that vulnerabilities fixed during a previous release roll into the current software build, and the CDT must plan for regression testing to occur during the subsequent government verification event. This approach requires effective configuration management, vulnerability documentation, and tracking.

Requirements and Attack Surface Analysis – Since software intensive systems are often COTS-based IT systems, Phases 1 and 2 analyses may rely heavily on RMF artifacts. If system requirements have not changed for each incremental delivery and the threat assessment is also unchanged, then cybersecurity testers may not need to repeat Phase 1. The CDT should reexamine the system’s attack surface for new connections and external interfaces with each incremental delivery. For extraordinary cases, it may be possible to merge Phases 1, 2, and 3 relying heavily on RMF artifacts and security controls testing plus the VOLT report to ensure a threat viewpoint is included for test planning. Contractor led security controls testing may be an option in extreme cases, but government cybersecurity T&E should monitor test results.

Vulnerability Assessments – Phase 3 testing is most intensive during the first increment delivered, and then each subsequent release focuses on the differences and the interfaces with the changes. Tailor CVI test activities for each software delivery. Buying COTS software does not imply that the system is inherently resilient, since all COTS systems use customized configurations once implemented. Adversaries are also able to purchase the system, use the same customized configuration, and use the duplicated system to research exploitable vulnerabilities, without informing the COTS system developer. Testing is still required to ensure configurations function as intended. The CDT ensures documentation and tracking of vulnerabilities is occurring, especially with COTS, and schedule recurring software and

---

4 DoD Instruction 5000.02, Model 2: Defense Unique Software Intensive Program, (September 14, 2017).
interface testing (Phase 3) based on the software build and build upon previous tests. The CDT also conducts Phase 5 testing as described in the main body of this guidebook or plan to use integrated testing to gather the OTA desired data during Phase 3 events.

**Threat-Based Testing** – The CDT conducts Phase 4 and Phase 6 testing as described in the main body of this guidebook. Since software intensive systems rely heavily on COTS, they provide well-known avenues for adversaries to breach the system and then move to other critical DoD systems via system interfaces. Threat-based testing supplements the RMF SCA and informs the ATO process. The CDT should conduct separate, not integrated, Phases 4 and 6. Integrating Phases 4 and 6 results in threat-based cybersecurity testing occurring only during OT&E and eliminates the ability to inform MS C, OTRR, and the ATO regarding discovered mission impacting vulnerabilities. The PMs should allow adequate resources to fix exploited vulnerabilities prior to system fielding or deployment.

**C.4.1 Incrementally Deployed Software Intensive Systems**

Incrementally deployed software intensive systems as described in DoDI 5000.02, Model 3 include systems software where deployment of the full capability will occur in multiple increments as new capability is developed and delivered ideally during 1- to 2-year cycles. This model differs from Model 2 by the rapid delivery of capability through multiple acquisition increments, each of which provides part of the overall required capability to achieve initial operational capability. Agile software development techniques may also be used to deliver rapid, limited, capability drops (CD1 through CDn) to end users compared to capabilities delivered in a less frequent software increment. Requirements modifications may occur with delivery of individual features as end users get a better idea of the end-result of the capability they requested in the initial requirements. Figure C-2 illustrates this model.

![Incrementally Deployed Software Intensive Systems Diagram](image)

**Figure C-2. Agile Release Cycle**

**Requirements and Attack Surface Analysis** – It may be possible to conduct Phase 1 and 2 analyses once for the entire software system. If software sprints and deliveries to end users create new requirements and functionality, repeat Phase 1. Requirements may change through software delivery

---

5 DoD Instruction 5000.02, Model 3: Incrementally Deployed Software Intensive Program, (September 14, 2017).
sprints. The Phase 2 analysis encompasses the overall architectural design of the system to expose any inherent vulnerabilities that may not be obvious at the individual capability/feature level. When capability delivery introduces communication and component-level changes to the system, attack surface analysis should be repeated.

**Vulnerability Assessments** – Phase 3 test activities include oversight of contractor cybersecurity T&E and/or customer involvement in verifying functionality for each incremental capability delivery. If agile software development is planned, government Phase 3 software testing and interface testing schedules are based on a release schedule with a focus on each capability drop (CD). The first CD undergoes Phase 3 and 5 testing and the interim CDs undergo Phase 3 testing. Each recurring test for individual features should build upon previous tests and verify fixes of previous test results. Phase 5 testing is needed as part of OT&E as described in Model 3, but Phase 5 testing is performed only with the final CD and is not repeated for each agile capability drop. If there are changes to the release schedule and capabilities for CDs, the CyWG should assess the risk of adding more testing (e.g. Phase 5 and 6 could be performed on an interim CD).

**Threat-Based Testing** – It is not necessary to perform Phase 4 for each agile build. The first and interim CDs undergo Phase 4 testing. The CDT may also schedule Phase 4 ACD periodically when a feature delivery encompasses and/or modifies the architecture such as when new interfaces are added. An MBCRA/CTT exercise can help to identify the components of the architecture that are at risk for exploitable vulnerabilities that persist with each CD. Phase 6 testing is needed as part of OT&E as described in Model 3, but Phase 6 testing is essential only with the first and final CDs. Phase 6 does not need to be planned for each agile build.

Combining Phases 3 and 4 is not recommended. The purpose of Phase 3 is not solely to provide reconnaissance for Phase 4. Phase 3 can be performed quickly for the small increments developed by an agile process. PMs do not need to resource two different test teams or test infrastructures during DT&E to perform Phases 3 and 4. An NSA-certified Red Team is not needed for Phase 4 when the system is not connected to the DoDIN.

**C.5 Small Program Considerations**

Smaller ACAT programs (e.g., ACAT 2, 3, and below) and acquisition programs that are not ACAT programs can tailor the cybersecurity T&E phases, but this tailoring guidance applies to stand-alone (e.g., programs not affiliated or connected with larger acquisition programs). If integrating with a larger system, such as platform IT, the smaller system needs to leverage the activities of the larger system as an enterprise cybersecurity testing approach based on the needs of the larger system. If small systems are starting after MS B or post-contract award, then the guidance for compressed timeframe systems may also apply.

**Requirements and Attack Surface Analysis** – Small systems may be able to rely more heavily on RMF artifacts due to a reduced number of sub-systems and interfaces with multiple systems. It may be possible to conduct Phase 1 and 2 analyses in parallel based on RMF artifacts. If multiple software releases to end users create new requirements, consider repeating Phase 1. The Program VOLT report if available, should supplement RMF artifacts to include threat-based analysis. Conducting an MBCRA may help small test organizations move quickly through Phases 1 through 3 by concentrating testing on potentially mission-impacting vulnerabilities identified during the CTT.

**Vulnerability Assessments** – Cybersecurity DT&E iteratively performs verification of all implemented security controls and performance parameters as part of Phase 3 testing to find and fix vulnerabilities before the formal security controls assessment. This process provides test data that satisfies RMF requirements. Small systems may also integrate the vulnerability testing performed during Phases 3 and 5 and collect test data that also satisfies RMF requirements. The combined events occur before MS C or
initial fielding if there is not MS C. PMs must ensure that the data they need to assess Phase 5 in an operational environment is included in the test planning and that there is agreement on a suitable test environment to satisfy all test requirements (e.g., informing the ATO if needed, degree of operational realism needed, etc.). If the contractor is required to perform Phase 3 testing and the test results are sufficient, the system could move directly into government verification testing (Phase 5) in the operational environment.

**Threat-Based Testing** – Perform adversarial testing as early as possible in lab environments or in the National Cyber Range. Do not combine or integrate Phases 4 and 6.

### C.6 DoD Cloud Computing Platforms

FedRAMP is a Federal government program focused on enabling security capabilities for cloud computing for the Federal government. Due to its warfighting mission, DoD has unique information protection requirements that extend beyond the controls assessed via FedRAMP. The DoD Cloud Computing Security Requirements Guide (SRG)\(^6\) outlines the security controls and additional requirements necessary for using cloud-based solutions within the DoD. DoD Mission owners who plan to deploy their applications into the cloud must follow the DoD Cloud Computing SRG guidance and the additional requirements it levies beyond those imposed by FedRAMP. CDTs and OTAs must be familiar with this guidance when planning for testing in commercial or government-provisioned FedRAMP and DoD cloud environments.

Mission owners select Cloud Service Operators (CSOs) and Cloud Service Providers (CSPs) from the DoD Cloud Service Catalog based on the security posture needed and their risk tolerance. The SRG defines the security requirements for DoD’s use of cloud computing. It covers several areas:

- Security requirements for CSP’s service offerings.
- Security requirements for assessing commercial and DoD CSPs for inclusion in the DoD Cloud Service Catalog.
- Security requirements for Mission Owner’s systems/applications instantiated on various cloud service platforms.

CDTs and OTAs should plan testing based on knowing the CSP-implemented security controls and features, and the security controls that are the responsibility of the system under test. CDTs and OTAs should be aware that the separate areas of responsibility may likely require different testing strategies. The assessed security features in the system are highly dependent on the cloud computing platform chosen by the Program Office. CDTs and OTAs should understand the cybersecurity risks associated with what testing can and cannot be accomplished when deploying to a cloud and should document the testing plan and associated risks in the TEMP. The participation of CyWG members with subject matter expertise in the specific CSO is essential to test planning and execution.

**Requirements and Attack Surface Analysis** – Phase 1 analysis should include an analysis of cloud computing service types that the system will be using. The current threat environment associated with CSPs and threat tactics are essential to understanding where to focus Phase 1 and 2 analyses. The common options are Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). The cloud service options selected will inform the required controls and assessment of the controls. Testers must understand the proposed system design and its integration into the chosen cloud service type.

---

Phase 2 attack surface analysis should encompass the CSP’s service and architecture as much as possible, since security features, and who is responsible for implementing them, are dependent on the service type the system will use. In all cloud service types, responsibility for system security is shared between the DoD mission owner, the CSO, and the CSP. Special emphasis should be given to any area where CSP and DoD mission owner responsibility overlap, such as customer configurable portions of the CSO. This overlap of responsibility can lead to omissions in implementation of system security requirements resulting in avoidable vulnerabilities. Figure C-3 illustrates this concept of shared responsibility. The Mission Owner inherits security features from the CSO, which the CSP implements and maintains.

- Mission Owner systems or applications built on an IaaS or PaaS offering will be subject to meeting many of the same security controls within the system/application.
- Mission Owners contracting for SaaS offerings inherit the bulk of compliance with the security controls from the CSO.

Figure C-3. Notional Division of Security Inheritance and Risk

Vulnerability Assessments – Cybersecurity Testers test the system in an integrated and emulated environment before moving to the cloud environment. If system development is being done in the cloud, the ideal test environment would be an exact virtual instance of the system under test, including the hosting environment. Cybersecurity testers should request the current test results applicable to their system from the CSP for each cloud service type. The Cloud Security SRG describes this process. The test results may indicate immediate remediation and retesting of the system is needed based on security issues and deficiencies discovered in the CSP service.

Threat-Based Testing – CSPs follow FedRAMP Penetration Test Guidance that applies to the cloud service type infrastructure. This guidance provides guidelines for organizations regarding planning and conducting penetration testing and analyzing and reporting on the findings. The SRG describes the FedRAMP CSO and CSP required testing for attack vectors; however, some attack vectors may not be applicable.

CDTs request penetration test findings from the CSP or from the ISSM and AO. The penetration testing covers only the CSO infrastructure. Therefore, the CDT must plan for Phase 4 adversarial testing on the system under test before integration into the cloud service. Systems using cloud services should consider...
Considerations for Tailoring the Cybersecurity T&E Phases

Cybersecurity Test and Evaluation Guidebook 2.0

the use of a cyber range for testing since CSPs do not typically allow test programs to execute penetration testing on their servers. Another option CDTs should investigate is that in some cases, the CSP may also provide a test platform for the system under test as a virtual instance in the same platform as the production instance. The scope of Phase 4 activities performed after integrating the system into the cloud service is dependent on the type of cloud service used.

**C.7 Defense Business Systems Using the Business Capability Acquisition Cycle**

Defense Business Systems that are not designated as a MDAP use the BCAC for business systems requirements and acquisition, described in DoDI 5000.75. Figure C-4 shows the cybersecurity T&E process mapped to the BCAC process.

DoDI 5000.75 states that the acquisition program’s implementation plan must include cybersecurity processes to reduce technical risk through T&E management requirements including:

- DEF
- Cooperative vulnerability identification and adversarial cybersecurity testing in both developmental and operational test
- A CEVA as outlined in the January 21, 2015, DOT&E Memoranda – CEVA is required only for DoD systems whose functions include financial or fiscal/business activities or the management of funds.
- Direction to MDAs to avoid tailoring cybersecurity T&E solely to meet ATO requirements

Table C-3 shows the BCAC acquisition decisions informed by cybersecurity T&E.

**Table C-3. BCAC Acquisition Decisions Informed by Cybersecurity T&E**

<table>
<thead>
<tr>
<th>Cybersecurity T&amp;E Functions</th>
<th>Cybersecurity T&amp;E Phase</th>
<th>DoDI 5000.75 Decision and Review Points Influenced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early Cybersecurity Tester Involvement Activities</td>
<td>Phase 1</td>
<td>BCAC Solution Analysis ATP and Functional Requirements ATP</td>
</tr>
<tr>
<td>DT&amp;E/OT&amp;E Planning Activities</td>
<td>Phase 2, 3</td>
<td>BCAC Functional Requirements ATP, Draft RFP, Acquisition ATP</td>
</tr>
<tr>
<td>DT&amp;E Test Execution Activities</td>
<td>Phase 3, 4</td>
<td>BCAC Limited Deployment ATP(s)</td>
</tr>
</tbody>
</table>

C-10

Considerations for Tailoring the Cybersecurity T&E Phases
Considerations for Tailoring the Cybersecurity T&E Phases

<table>
<thead>
<tr>
<th>Cybersecurity T&amp;E Functions</th>
<th>Cybersecurity T&amp;E Phase</th>
<th>DoDI 5000.75 Decision and Review Points Influenced</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT&amp;E Test Execution Activities</td>
<td>Phase 5, 6</td>
<td>BCAC Full Deployment ATP</td>
</tr>
</tbody>
</table>

DBS’ share some characteristics with software intensive systems due to using COTS products.

**Requirements and Attack Surface Analysis** – If DBS programs select an IT solution, cybersecurity testers should conduct Phases 1 and 2 analyses to inform the ATPs shown in Table C-3. Since DBS systems often employ traditional IT components, Phase 1 and 2 analyses may rely heavily on RMF artifacts. It may be possible to merge Phases 1, 2, and 3 relying heavily on RMF artifacts and security controls testing.

**Vulnerability Assessments** – DBS programs conduct Phases 3 and 5 to inform ATO and BCAC Limited Deployment ATP decisions. Using COTS products does not imply that the IT system is inherently resilient to cyber threats, since all COTS systems use customized configurations once implemented, and system adversaries are also able to purchase the system, configure it in the same way and find new exploitable vulnerabilities without informing the developer. Phase 3 testing is required to ensure configurations function as intended without a high risk of compromise. The CDT should ensure documentation and tracking of vulnerabilities and use publicly available vulnerability databases to ensure discovery and remediation of known vulnerabilities prior to system deployment. DBS programs may consider integrating Phases 3 and 5 when feasible or where testing timelines are compressed, as described in Section C.4.

**Threat-Based Testing** – DBS programs conduct separate Phase 4 and Phase 6 testing to inform the Limited Deployment ATP and the Full Deployment ATP decisions. Since DBS programs rely heavily on COTS, they provide well-known avenues for adversaries to breach the system and then move to other critical DoD systems via system interfaces. DBS programs should allow adequate time to fix Phase 4 exploited vulnerabilities in COTS prior to system deployment. DBS programs may consider integrating Phases 4 and 6 when feasible.
Appendix D  Key System Artifacts for Cybersecurity T&E Analysis and Planning

The following guidance for the CDT and the test team on the analysis and use of system artifacts for T&E. All explanations are from the Defense Acquisition University Guide or from references in Chapter 11.

**Anti-Tamper (AT) Plan** – This document covers developing and communicating a system’s AT protection throughout its life cycle. It includes the CPI (organic and inherited) criticality and protection level, the system’s AT concept, AT protection solution set and implementation description, the AT evaluation plan, and the key management plan, as applicable based upon the maturity of the system. The AT plan is an appendix to the Program Protection Plan.

**Attack Surface Analysis Report** – The purpose of an Attack Surface Analysis Report is to provide guidance on the risk areas of an attack surface for a system. This will make developers and security specialists aware of what parts of the application are open to attack and help them find ways to minimizing this. Security architects and penetration testers usually perform the Attack Surface Analysis but developers must understand and monitor the Attack Surface as they design, build, and change a system. An Attack Surface Analysis Report can also help to:

- identify the functions or parts of the system need to be reviewed/tested for security vulnerabilities
- identify areas of code that require extra protection
- identify changes in the attack surface that need a threat assessment

**Capability Development Document (CDD)** – The CDD captures the essential information to develop a proposed system. It outlines what the useful, logistically supportable, and technically mature capabilities will be. The document supports a Milestone B decision review. The purpose of this document is to provide the sponsor with authoritative, measurable, and testable capabilities that the warfighter will need. The CDD must include a description of the Doctrine, Organization, Training, Material, Leadership and Education, Personnel, and Facilities as well as the policy impacts and constraints.

**Capability Production Document (CPD)** – The CPD outlines capability requirements in terms of Key Performance Parameters, Key System Attributes, Additional Performance Attributes, and other relevant information to support production of a material capability solution. The PM needs a validated CPD for each milestone acquisition decision. The CPD identifies, in threshold/objective format, the specific attributes that contribute most significantly to the desired operational capability.

**Concept of Operations (CONOPS)** – A CONOPS is a user-oriented document that describes systems characteristics for a proposed system from a user's perspective. A CONOPS also describes the user organization, mission, and objectives from an integrated systems point of view and is used to communicate overall quantitative and qualitative system characteristics to stakeholders.

**Cyber Survivability Endorsement Implementation Guide (CSEIG)** – Cybersecurity Survivability Risk Category (CSRC) – Joint programs that include a SS KPP in their system requirements must include an assessment of cyber survivability in their assessment of the SS KPP. The CSEIG provides the guidance for developing the CSRC contained in the acquisition program’s CDD and other requirements documents. Acquisition programs should refer to the CSEIG for further information on the CSRC process.

**Cybersecurity Strategy** – The PM prepares the Cybersecurity Strategy and appends it to the PPP. The DoD or Component CIO should approve the strategy before T&E organizations incorporate it. The Cybersecurity Strategy includes cybersecurity and resilience 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 CDT should make sure the Cybersecurity Strategy is referenced and coordinated in the TEMP. The Cybersecurity Strategy provides input for the requirements for vulnerability and adversarial testing.

Cybersecurity Service Provider (CSSP) – The CSSP Support Plan is not an official document, but describes the alignment of a system with its CSSP. The CSSP describes how the service provider will provide computer network defense activities for the system.

DBS Capability Support Plan – The capability support plan documents the roles and responsibilities for sustainment activities. It includes:

- A governance structure that provides resources, prioritizes changes, and approves implementation plans for changes that fall within scope of the original capability requirements.
- A threshold for changes to determine whether the change requires a new BCAC initiative. Major capability changes that do not fall within the scope of the original capability requirements will require re-initiation of the process.
- Plans for conducting a post-implementation review.

DBS Design Specifications – Design specifications are based upon the high-level requirements established during functional requirements definition. This includes the functional requirements, along with associated inputs and outputs for the functional requirements, and associated technical and life cycle support requirements. Design specifications are not a specific document. Instead, they are the content that the Program Office needs to specify the design of the business system and that the system stores and uses in the applicable format or repository.

DBS System Functional Requirements – Functional requirements describe how the business system will achieve the future business processes. Functional requirements include enough detail to inform definition of potential business system solutions and evaluation criteria, but without including too much detail that would overly constrain solution selection.

DoDAF Operational and System View – DoDAF-described Models in the Operational Viewpoint describe the tasks and activities, operational elements, and resource flow exchanges required to conduct operations. The OV DoDAF-described Models may be used to describe a requirement for a “To-Be” architecture in logical terms, or as a simplified description of the key behavioral and information aspects of an “As-Is” architecture.

The DoDAF-described Models within the Systems Viewpoint describes systems and interconnections providing for, or supporting, DoD functions. DoD functions include both warfighting and business functions. The systems Models associate systems resources to the operational and capability requirements. These systems resources support the operational activities and facilitate the exchange of information.

Information Support Plan (ISP) – An information set supporting interoperability test and certification. It identifies and documents information needs, infrastructure support, and IT and National Security Systems interface requirements and dependencies focusing on net-centric, interoperability, supportability, and sufficiency concerns. It is a requirement for all Information Technology acquisition programs, including National Security Systems, that connect in any way to the communications and information infrastructure.

Initial Capabilities Document (ICD) – The ICD documents one or more new capability requirements and associated capability gaps. The ICD also documents the intent to partially or wholly address identified capability gaps with a nonmaterial solution, material solution, or some combination of the two. An ICD may lead directly to a CPD.

Mission-Based Cyber Risk Assessment (MBCRA) – See Appendix X3 for information.
Operational Test Readiness Review (OTRR) – The OTRR is a multi-disciplined product and process assessment to ensure that the system can proceed into IOT&E with a high probability of success, and that the system is effective and suitable for service introduction. The OTRR is complete when the Service Acquisition Executive evaluates and determines material system readiness for Initial Operational Test and Evaluation.

Program Protection Plan (PPP) – The PPP is a living plan to guide efforts to manage the risks to CPI and mission critical functions and components and system information. This milestone acquisition document captures both systems security engineering (SSE) and security activities and the results of the analyses as the system become more defined.

Security Plan – The RMF Security Plan is reviewed as part of the first phase of cybersecurity T&E to assist in understanding cybersecurity and resilience 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 CDT should review Security Plan with 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.

Security Assessment Plan – It is highly recommended that the CDT include the SCA within the CyWG and reference the RMF Security Assessment Plan within the TEMP. The Security Assessment Plan describes the PM’s plan to assess the security controls. The CDT should coordinate with the SCA to align development of the RMF Security Assessment Plan with development of the TEMP. The security controls assessment is coordinated with developmental test events defined in the TEMP.

As the Security Assessment Plan is developed, the CDT should review the selected security controls, the order in which the security controls will be implemented, and who is responsible for security control assessment. 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 CDT should coordinate with the PM 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 noncompliant 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 CDT and DT&E, for systems under oversight, should use the Security Assessment Report as one input to their assessment of developmental test results and risk.

System Design Documents – The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces. This includes items such as the contractor system designs, wiring diagrams, the SEP, etc.

System Engineering Plan (SEP) – The Systems Engineering Plan is a living document that details the execution, management, and control of the technical aspects of an acquisition program from conception to disposal. The SEP outlines how the systems engineering process is applied and tailored to meet objectives for each acquisition phase. The SEP is updated as needed to reflect technical progress achieved to date and to reflect changes in the technical approaches stemming from the findings and results of the technical reviews, program reviews acquisition milestones, or other acquisition program decision points.
Key System Artifacts for Cybersecurity T&E Analysis and Planning

**System Requirements Document (SRD)** – The System Requirement Document (SRD) defines system-level functional and performance requirements for a system. The SRD, which the Program Office develops, is derived from the CONOPS, system-level performance metrics, mission threads/use cases, and usage environment. It includes a system level description of all software elements that the preferred system concept requires.

**Testing & Evaluation Master Plan (TEMP)** – The TEMP documents the overall structure and objectives of the Test and Evaluation (T&E) program and articulates the necessary resources to accomplish each phase of the test. It provides a framework within which to generate detailed T&E plans and documents schedule and resource implications associated with the T&E program. The TEMP also identifies the necessary DT&E, OT&E), and Live Fire Test and Evaluation (LFT&E) activities, and provides a clear roadmap connecting evaluation objectives, test measures, requirements, test methodologies, decision points, test events, and resources.

**Validated On-Line Threat (VOLT) report** – The VOLT report provides an assessment of a potential adversary’s ability to neutralize or degrade a system under development. It summarizes the approved threat profile for combat and materiel developers, developmental and operational testers, and evaluators for all systems. The VOLT report is the authoritative threat assessment tailored for and focused on one specific ACAT I, II, or III program and authorized for use in the Defense Acquisition Management process. VOLT reports include system-specific CTMs from the DITL and provide a discussion of each module’s relevance to a specific acquisition program or planned capability. The DITL is a collection of threat modules that address threat capability developments in the next 20 years in a specific topic area, such as electronic warfare, air-to-air missiles, early warning radars, laser weapons, cyberwarfare, and adversary tactics.

The DITL is described here:

Cyber threat libraries are available here:
- (U) SIPR - [https://intellipedia.intelink.sgov.gov/wiki/Defense_Intelligence_Threat_Library](https://intellipedia.intelink.sgov.gov/wiki/Defense_Intelligence_Threat_Library)
Appendix E  Guidance for the Cybersecurity Portion of the DEF

E.1 Introduction and Purpose

One key aspect of required T&E documentation is the DEF. The DEF guides development of the DT&E strategy by identifying the critical acquisition program decisions and defining the test data needed to inform the decisions. The DEF has four major areas, including cybersecurity. The purpose of the cybersecurity portion of the DEF is to depict the test events that will generate the information needed to inform the acquisition program’s key decision points regarding DSQs within the system cybersecurity capabilities, and the technical measures used to quantify the system cybersecurity capabilities. Cybersecurity is an integral part of the DEF.

E.2 Schedule

The developmental evaluation methodology, including cybersecurity capabilities, must be considered during MS A. Cybersecurity developmental efforts for Phase 1 and Phase 2 inform the planning for the MS B TEMP, RFP, and CDD. Mission-based cybersecurity risk assessments performed during Phase 1 and Phase 2 also inform the identifying of the test events included in the DEF for MS B.

MS B requires a TEMP with a DEF. Data collected during Phase 1 and Phase 2 is leveraged to identify cybersecurity tests, which results in efficiency and cost reduction. The DEF-identified test events also require planning to accommodate resources necessary to conduct testing. By doing so, the Program Office can begin the planning process to ensure that resources are available at the time of testing. For example, the National Cyber Range may require up to a year of coordination before a test event can occur. The DEF at MS B identifies tests to gather the key data from Phase 3 and Phase 4 test events within cybersecurity capabilities that support assessing:

- CTPs and system technical specification
- Resiliency
- Data security

MS C includes TEMP updates, including DEF updates, if additional cybersecurity DT&E is necessary after MS C. DEF identified test events should leverage the findings from Phase 3 and Phase 4 testing. The scheduled DEF activities are shown in Figure E-1.

![Figure E-1. DEF Schedule](image-url)
E.3 Format

DAG Chapter 8-3.7.2.2 and DoDI 5000.02, Enclosure 4 provide guidance on the DEF and its inclusion in the TEMP. This information is put into a matrix format, as shown in Figure E-2. The DEF covers cybersecurity along with the three other areas: performance, interoperability, reliability; a separate cybersecurity evaluation framework is not required for the TEMP. The main components of the DT&E strategy and the DEF are:

- **Decisions**: Decision points throughout the acquisition life cycle that decision makers—from the PM to the MDA—determine and that the DT&E-gained knowledge has informed. The decisions may change with each TEMP update.
- **DSQs**: Questions capturing the essence of the information needed to make informed decisions.
- **Developmental Evaluation Objectives**: The system’s performance, interoperability, cybersecurity, and reliability capabilities to be evaluated. For cybersecurity, the PM defines the capabilities that will be evaluated to answer the DSQs. For example, data security both within the system boundary and across interfaces and system or mission resiliency are examples of cybersecurity capabilities.
- **Description**: The testable technical measures or attributes within each capability area. For cybersecurity, the technical attributes for evaluation are typically prevent, mitigate, and recover.
- **Data Sources**: The test, modeling, and simulation, or other events generating the data needed for system evaluation. For cybersecurity, these events include:
  - Analysis assessment activities such as architecture vulnerability assessment, criticality analysis, and MBCRAs
  - Cooperative vulnerability identification events to include contractor test activities, controls assessments, vulnerability scanning, and penetration testing
  - Adversarial DT&E events
Staffing and Participation

The DEF Core Team consists of the Program Office acquisition, engineering, and test experts across the functional evaluation areas captured in the DEF and any other developmental oversight organization representatives. A small, focused group (about 8-10 people) including the functional subject matter experts is required to ensure that the Core Team is most effective in building the DEF in the shortest period. The Program Manager, Chief Engineer, Chief Developmental Tester, Lead Developmental Test and Evaluation Organization Lead, and CyWG representative lead the DEF development as follows:

- Program Manager – provides a brief description of the acquisition strategy, from which the discussion develops the acquisition decisions and DSQs; provides the decision-making expertise throughout the discussion.
- Program Chief Engineer – defines the capabilities and top-level requirements that will be used to measure/evaluate the performance and provides the capabilities expertise throughout the discussion.
- Chief Developmental Tester – understands the decision making and evaluation purpose of the DT&E strategy, uses the Developmental Evaluation Framework in leading the DT&E execution.
- Lead Developmental T&E Organization representative – understands purpose of testing events, defines test and M&S events, and provides the test/M&S expertise throughout the discussion.
- CyWG Representative – observes and learns the system functional capabilities used to measure/evaluate performance of the system and how security capabilities are associated with the functional capabilities.
The cybersecurity portion of the DEF is developed at the same time as the rest of the DEF. Program leadership involvement is required to ensure the technical performance, interoperability, and reliability measures can be linked to the cybersecurity testable attributes for cybersecurity-driven assessments. The development of the cybersecurity portion requires representation from the CyWG (discussed in Section 3.1.5).

The cybersecurity portion of the DEF aligns the test schedule with the information needed by decision makers at significant decision points, captures cybersecurity capabilities needed to support the mission performance, provides a framework to plan cybersecurity test activities, and guides and informs cybersecurity developmental test planning.

E.5 Cybersecurity DT&E Objectives

In accordance with DoDI 5000.02 Enclosure 4, a robust DT&E program includes many key activities to provide the data and assessments for decision making. The objective of cybersecurity DT&E is to identify issues before MS C that are related to the resilience of military capabilities from cyber threats. Early discovery of system vulnerabilities can facilitate remediation and reduce the impact on cost, schedule, and performance.

The DT&E program populates the DEF with test events to provide supporting decision data needed to:

- Verify achievement of critical technical parameters and the ability to achieve key performance parameters, and assess progress toward achievement of critical operational issues.
- Assess the system’s ability to achieve the thresholds prescribed in the capabilities documents for cybersecurity requirements, if any.
- Provide data to the PM to enable root cause determination and to identify corrective actions.
- Include T&E activities to detect cybersecurity vulnerabilities within custom and commodity hardware and software.
- Stress the system within the intended operationally relevant mission environment.
- Support security control assessment for the RMF assessment and authorization process.

E.6 DEF Development Tasks

When developing the cybersecurity portion of the DEF, the DEF Core Team, with support from the CyWG, uses the DEF Core Team-defined DSQs for the following tasks:

- **Task 1**: Define security capabilities and quantifiable cybersecurity technical measures to address during testing.
- **Task 2**: Determine the evaluation data needed to support the acquisition program decision points.
- **Task 3**: Determine the test activities needed to produce the desired data.
- **Task 4**: Incorporate test activities into test events and document in the TEMP.

**Task 1** includes defining security capabilities that align with the system performance capabilities. One way of accomplishing this is to understand how a cyber-attack could impact the mission objectives if the data required to execute the mission objectives become altered, unavailable, or exploited in advance of mission execution. Examples of security capabilities are data security and system resiliency.

Task 1 also defines the technical measures or attributes associated with each of the security capabilities, such as prevent, mitigate, and recover. Prevent actions protect the system’s functions from the most likely and greatest risk of cyber threats. Mitigate actions detect and respond to cyber-attacks, enabling system resiliency. Recover actions ensure minimum cybersecurity capability available to recover from cyber-attack and enable the system to restore full functionality quickly.
Figure E-3 shows security capabilities and technical measures in Section 1. The CyWG can partially perform this task in advance of the DEF Core Team session using any findings and analysis from mission-based cyber risk assessments.

**Task 2** includes identification of evaluation data needed to support the DSQs. Evaluation data needed is discovered by examining the system specifications, PPP, Cybersecurity Strategy, RMF Security Plan, OT data requirements, mission CONOPS, mission threads, and Phase 2 results. Needed evaluation data comes from testing the interfaces, components, and system planned. Before test events are identified and entered in the DEF, the PM must identify the scope of testing. The CyWG representatives may attend the DEF Core Team session prepared with planned test objectives, or the CyWG may perform this task after the DEF Core Team session. The data is not included in the DEF; it is used to complete the next task.

**Task 3** includes identification of the test events that will produce the evaluation data. See Figure E-3 for the test events in Section 3.

**Task 4** of the cybersecurity DEF engagement is to include the DEF into the TEMP. All the testing events annotated within the DEF will be described fully within the body of the TEMP. Each test event maps to testing organizations, test resourcing estimates (people, test items, tools, ranges, funding), test dependencies, and test schedule.

Figure E-3 shows a completed cybersecurity portion of the DEF.
<table>
<thead>
<tr>
<th>Developmental Evaluation Objectives</th>
<th>System Capabilities (SRD Rqmts)</th>
<th>Technical Measures</th>
<th>EMD RFP Release</th>
<th>MS B / Contract Award EMD Long Lead items for A/C (A1, A2, A3) &amp; Radars (for A/C and SIL)</th>
<th>Approval to Enter Gov’t Led IDT&amp;E</th>
<th>LRIP Long Lead Items</th>
<th>Approval to Enter IOT&amp;E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect; Data Security - Systems</td>
<td>Data at rest, Data in transmission</td>
<td>Architectural Vulnerability Analysis (AVA)</td>
<td>Mission Cyber Dependency Analysis - Cyber Table Top Exercise</td>
<td>CVI - Data Security testing, CVI - STIG compliance verification</td>
<td>Security Controls Assessment (SCA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect; Data Security - Interfaces</td>
<td>Critical Data Exchanges</td>
<td>Architectural Vulnerability Analysis (AVA)</td>
<td>Interoperability - Cybersecurity ft</td>
<td>CVI - CTT Verification Exercise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Resilience and Survivability</td>
<td>SS KPP CSA Detecting attacks (how long to detect, how many detected versus attempted, mission impacts)</td>
<td>Mission Cyber Dependency Analysis - Cyber Table Top Exercise</td>
<td>CVI - Cyber Functionality Verification</td>
<td>CTT Verification Exercise</td>
<td>ACD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS KPP CSA Responding to attacks (how long to respond)</td>
<td>Mission Cyber Dependency Analysis - Cyber Table Top Exercise</td>
<td>CVI - Incident Response Assessment</td>
<td>ACD</td>
<td>ACD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS KPP CSA Recovering from attacks (how long does recovery take? Does that impact success of the mission?)</td>
<td>Mission Cyber Dependency Analysis - Cyber Table Top Exercise</td>
<td>CVI - COOP assessment</td>
<td>ACD</td>
<td>ACD</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix F  Considerations for Staffing Cybersecurity T&E Activities

F.1  Introduction

The purpose of this appendix is to assist the Program Manager (PM) and Chief Developmental Tester (CDT) with identifying cybersecurity T&E personnel resources to enable successful planning and execution of cybersecurity T&E as described in this guidebook. Not only are the right resources required to perform the planning, but the PM must identify the right resources to execute testing and initiate the scheduling and collaboration with those organizations as early as possible.

F.2  Cybersecurity T&E Roles and Suggested Minimum Qualifications

No two systems or potentially test events, will require the exact same cybersecurity T&E, therefore the PM and CDT should carefully consider the skills and knowledge of the personnel supporting the system for cybersecurity T&E. Cybersecurity T&E personnel should have experience in the protocols and architecture associated with the system under test. For example, if the system under test is a world-wide-web (WWW)-based platform using COTS based software and hardware, then the cybersecurity testers should have previous experience with both WWW-based platform testing as well as the specific COTS product. On the other hand, if the system under test is an industrial control system with non-Internet Protocol (IP)-based communication, then the desired cybersecurity testers should have prior experience in industrial control systems.

Before selecting personnel to support testing, CDTs must understand the system design and the technologies the system uses, including system interfaces. This analysis is performed during Phases 1 and 2. The system design is the primary driver for selecting skilled personnel to perform testing. To assist in this analysis the CDT should first enlist a cybersecurity analyst or SME to be a member of the CyWG. The Cybersecurity Analyst or SME can work with the contractor/developer to first understand the system’s design and then determine the skills needed to test the system. This effort also informs test scheduling, tool and infrastructure planning (Appendix X4), as well as the threat characterization (Appendix X2).

The focal point for enlisting and coordinating cybersecurity T&E expertise is the CyWG. The CyWG is responsible for advising the CDT on the full range of cybersecurity T&E activities that will verify cybersecurity and resiliency capabilities for the system. The CyWG should ensure that cybersecurity T&E staff have the skills required to perform the test planning and test execution assigned to them. If the CyWG cannot recruit skilled staff from within the acquisition program to support cybersecurity T&E, acquisition programs may want to consider the following options;

- Consult with similar programs and/or PEO
- Borrow skilled staff from similar programs
- Send staff for training with similar programs
- Fund Systems Engineering and Technical Assistance (SETA) contractors to fill in gaps (independent from the acquisition contractor)
- Recruit FFRDC and/or UARC staff to supplement

F.2.1  Cybersecurity DT&E and OT&E Technical Experts

Cybersecurity DT&E and OT&E technical experts are a broad description of a class of experts specializing in analysis, planning and conducting cybersecurity T&E activities. Cybersecurity T&E technical experts include hands-on testers, analysts, assessors and technical SMEs in a variety of technical disciplines. The following section describes the roles typically needed to plan and conduct cybersecurity T&E and OT&E technical experts.
T&E. One person may fill more than one role, but each role brings a required focus area. Testing organizations may or may not already employ all the roles needed to support the variety of systems the organization tests. If a testing organization has a gap in the required cybersecurity T&E expertise to support system testing, then it may be possible to address the gap through partnerships or contracts with other organizations.

**F.2.1.1 Cybersecurity Analysts**

Cybersecurity Analysts examine architectures, controls, countermeasures, requirements, threats and the functional system and develop a view of the systems security posture that should be the subject of testing. Analysts consider assessment methods that are appropriate for the system, and ensure the chosen assessments align to test objectives. See Section 6, Table 6-2 of this guidebook for examples of different assessments that may be required. The system under test may be a sub-system, component, software, integrated components or architectures, networks and protocols. The Cybersecurity Analyst assists with planning all cybersecurity T&E using STAT to design a continuum of testing that matures with system development and reduces risk while assessing resiliency and survivability. The Cybersecurity Analyst helps ensure the correct scope of testing and the timing and frequency of testing while assisting the CDT with selecting the SMEs and other experts described below. The analyst assists with ensuring the program TEMP accurately reflects the testing, resources, and schedule for cybersecurity T&E activities. The Cybersecurity Analyst(s) supports:

- Analyzing cybersecurity requirements and characterizing the cyber-attack surface
- Planning and conducting mission-based cyber risk assessments
- Defining the scope of the government cybersecurity testing events and assessing the level of effort required to support and complete the cybersecurity testing
- Assisting the CyWG in capturing cybersecurity test event objectives for government and contractor testing
- Proposing the scope of contractor cybersecurity testing events to support government test objectives
- Supporting RMF security controls assessment
- Coordinating with the respective stakeholders for formal approval
- Working with the CyWG to ensure the event and report data are handled at the appropriate level if defined in a SCG
- Identifying the cybersecurity testing events appropriate to indicate in the DEF
- Providing input for cybersecurity evaluations
- Identifying the necessary resources and budget required to plan and perform testing events (technical experts, cybersecurity SMEs, test articles, tools, infrastructure, etc.)
- Advising on the cyber threat assessments

**Cybersecurity Analyst - Recommended Minimum Qualifications.** Cybersecurity Analysts should have the following minimum qualifications:

- Knowledge of organization's enterprise information security architecture system
- Knowledge of organization's evaluation and validation requirements
- Knowledge of an organization’s threat environment

---

8 Adapted from NIST and the National Initiative for Cybersecurity Education (NICE), *The National Workforce Cybersecurity Framework*
- Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])
- Knowledge of network hardware devices and functions
- Knowledge of systems administration concepts
- Knowledge of the systems engineering process
- Knowledge of penetration testing principles, tools, and techniques
- Familiarity with common tools utilized by attackers
- Experience with offensive security analysis tools and tactics
- Experience in designing a data analysis structure (i.e., the types of data the test must generate and how to analyze those data)
- Experience in determining an appropriate level of test rigor for a given system
- Experience in developing operations-based testing scenarios
- Experience in systems integration testing
- Experience in writing test plans

If Cybersecurity Analysts with the knowledge and skills needed are not part of the Program Office, the PM should resource support from either contractor service support (CSS), FFRDCs, UARCs, or the testing organizations that support DT&E and OT&E. Support from Cybersecurity Analysts is required beginning with Phase 1 activities and continuing through Phase 6.

F.2.1.2 Cybersecurity Subject Matter Experts

Cybersecurity SMEs provide expertise in specialized technologies such as specific operating systems, databases, software development methods, non-IP devices, network communications, and controls systems, etc. Select Cybersecurity SMEs with skills that align with the major design components of the system. In addition, ensure availability of relevant SMEs for specific COTS or GOTS testing. The SMEs must support planning and analysis activities to scope testing events and participate when the testing for their specialty area or component is in scope.

Cybersecurity Intelligence SMEs provide expertise on tactics of the threat adversary that are used during testing. Cybersecurity Intelligence SMEs understand the full suite of cyber-attack vectors and can help testers focus system tests on key cyber terrain that adversaries may target. These SMEs are needed to plan Phases 4 and 6 test activities.

Operational SMEs help cybersecurity testers understand how the system functions. SMEs may come from Program Offices, Intelligence, military personnel, R&D Organizations, vendors, National Laboratories, and other services. It is important for Cybersecurity SMEs to work closely with operational SMEs that thoroughly know the system from a design, functional and operational standpoint. These SMEs should participate in Phase 1-6 activities.

**Cybersecurity SMEs - Recommended Minimum Qualifications.** The SMEs and desired qualifications needed will vary from system to system, test to test. CDTs should take care in selecting SMEs to ensure they have the credentials and experience to support test design and execution based on the design components of the system.

F.2.1.3 Cyber T&E Leads for Developmental Testing

For Phases 1-4, the Lead Developmental Test Organization or the system’s government cyber DT&E organization who is resourced for cybersecurity DT&E, should provide a Cyber T&E Lead to the CyWG that will work closely with the Cybersecurity Analyst to develop the DT&E roadmap of contractor and government cybersecurity T&E events needed to evaluate the system’s cybersecurity, resiliency and survivability. The Cyber T&E Lead should plan government cybersecurity test events by recruiting the...
Considerations for Staffing Cybersecurity T&E Activities

The Cyber T&E Lead and the Cybersecurity Analyst should observe contractor test events, if possible, and review the detailed contractor test results to provide the CDT a technical analysis of the test and findings.

For each contractor or government developmental test event using a test range or test lab, a Cyber Test Event Lead (contractor, government, range) is responsible for leading the team of testers executing each event. The Cyber T&E Lead and the Cyber Test Event Lead work together in executing all developmental test events.

F.2.1.4 Cybersecurity Vulnerability Analysts

Cybersecurity Vulnerability Analysts (VAs) are hands-on testers who use both automated tools and other techniques to look for known vulnerabilities and attempt to exploit the vulnerabilities to understand likelihood and impact of the exposure. Typically, they are experts on Security Technical Implementation Guides (STIGs) for COTS and GOTS (when STIGs are defined), and they often function as both security controls assessors and vulnerability assessors. Cybersecurity VAs support Phase 3 and Phase 5 test activities and should participate in the CyWG. Some organizations refer to Cybersecurity VAs as either Blue teams or Green teams. Cyber VAs may provide test data to the PM for root cause determination to identify corrective actions.

Cybersecurity Vulnerability Analysts - Recommended Minimum Qualifications. The knowledge and recommended qualifications for Cybersecurity VA hands-on testers vary as with the Cybersecurity SMEs described in Section G.2.1.2 in terms of the protocols, architectures, and networks in scope for testing. The National Workforce Cybersecurity Framework, National Initiative for Cybersecurity Education (NICE), NIST Special Publication 800-181, provides a detailed list of recommended knowledge, skills and abilities for a variety of VAs within the Securely Provision work role. Additionally, a DoD cross-service high level set of recommended standards for Cybersecurity VA is under development. This appendix will be updated when the standards are published.

F.2.1.5 Cybersecurity Penetration and Adversarial Testers

Penetration and Adversarial Testers (PATs) are testers who specialize in testing using exploits and adversary tactics. Many times, the PAT teams are called Red Teams. These testers should be engaged with the CyWG when available beginning in Phase 2 and will also participate in MBCRAs to support test planning, and preparation for Phase 4 and Phase 6 test activities. The CDT should expect a team of PATs to be performing the testing for Phases 4 and 6.

Cybersecurity Penetration and Adversarial Testers – Recommended Minimum Qualifications. As with the Cybersecurity SMEs and the Cybersecurity VAs, the PATs selected to conduct testing for a system must have prior experience with the protocols, architectures, networks and interfaces associated with the systems under test. Below are the basic skillsets expected of a Penetration Tester:

- At least three years of related cybersecurity experience
- Familiarity and experience with common Operating Systems (OS) environments
- Familiarity with common tools utilized by attackers
- Experience with offensive security analysis tools and tactics
- Familiarity with tactics, techniques, and procedures utilized by attackers

---

10 Ibid
Considerations for Staffing Cybersecurity T&E Activities

- Familiarity with cybersecurity defenses (Intrusion Prevention System (IPS)/Intrusion Detection System (IDS), Firewalls, Security Information and Event Management (SIEM), etc.)
- Experience performing open source research
- Experience analyzing data from various sources of information and identifying potential vulnerabilities and attack vectors
- Familiarity with Python, Perl, or Ruby to craft custom scripts
- Operational understanding of TCP/IP and computer networking

F.2.1.6 Cybersecurity Red Team Organizations

Qualified Red Team organizations are used 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 cybersecurity by demonstrating the impacts of successful cyber-attacks and by demonstrating what works for the defenders (i.e., the CSSP) in an operational environment. Red Team organizations (not individuals) are certified by the NSA and accredited through U.S. Cyber Command to ensure they are able to transit DoD networks without doing harm to government systems.

*Red Team Testers - Recommended Minimum Qualifications.* Red Team organizations that are NSA-certified have specific certification requirements to achieve the certification from US Cyber Command. CJCSM 6510.03 describes Red Team certification and accreditation. As with the Cybersecurity SMEs and the Cybersecurity VAs, Red Team testers must have prior experience with the protocols, architectures, networks and interfaces associated with the systems under test. Their minimum qualifications are similar to Penetration Tester qualifications.

F.2.1.7 Cyber Test Range Representatives

Along with the Cyber Event Lead, Cyber Test Range Representatives assist the CDT with planning the test environments needed to conduct cybersecurity testing. Test Range Representatives work with the Cyber Event Lead to plan cybersecurity test infrastructure to support cybersecurity test events. They should have specialized technical knowledge and experience in building test environments to support cybersecurity testing. This includes a variety of skills and expertise, including knowledge of distributed testing, virtual environment emulation, network engineering, and knowledge of adversary access methods and tactics, and intelligence to generate effective range capabilities, characteristics, and scenarios. Cyber Test Range Representatives may recruit the following roles needed to plan and conduct cyber test events:

- **Event Planner/Coordinator** – Personnel responsible for ensuring cyber range capabilities meet their requirements. The Event Planner/Coordinator participates in event planning milestones and coordinates with all other planning roles to ensure required capabilities are provisioned for test events.11
- **Event Architect** - Personnel responsible for designing, implementing and validating cyber range event environments according to the event requirements. The Event Architect examines issues such as adequacy of bandwidth between distributed sites, potential stress and loading implications due to the event design, the baselines of the cyber range operating environment, and any necessary health and status monitoring required throughout the test event.12

---

12Ibid

Considerations for Staffing Cybersecurity T&E Activities
Range Engineer – Personnel who monitor, manage, operate, and/or create hardware, software, or networking elements of a cyber range to support the planned test events.\textsuperscript{13}

Security Engineer – Personnel who monitor, manage, and configure security devices and controls associated with cyber range events.\textsuperscript{14}

Cyber Test Range Representatives – Recommended Minimum Qualifications. The Cyber Test Range Representative should bring specific knowledge of high-fidelity, realistic cyber environments that can be used to conduct cyber testing during all phases of the system life cycle as well as testing of complex system-of-systems. If needed, National Cyber Range Complex (NCRC) SMEs are available through the TRMC to support the planning, execution, and analysis of test and training events. TRMC may further leverage available expertise from the Department of Energy, National Laboratories, and other sources as necessary and appropriate. Personnel fulfilling this role should have the following skills:

- Knowledge and understanding of the use of Live, Virtual, Constructive, Development and Evaluation (LVCDE) for conduct of cybersecurity T&E
- Knowledge and ability to design, deploy, and sanitize large-scale, high-fidelity test and training environments in which malicious threats can be released on operationally representative systems and networks to assess their impact
- Knowledge of the NCRC and other DoD cyber ranges and methods to collaborate test environments across cyber ranges using secure networks
- Knowledge of DoD test range capabilities and facilities awareness of other T&E facilities and resources, within and outside the DoD

F.2.1.8 Contractor Staff

Contractor staff are frequently the experts for the government systems they are building and therefore should be included in the CyWG. They supplement the knowledge of government design and test teams.

Contractor Representative Minimum Qualifications:\textsuperscript{15}:

- Knowledge and understanding of cybersecurity T&E methods, processes, and products
- Knowledge and understanding of cybersecurity principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and nonrepudiation
- Knowledge and understanding of risk management processes, including steps and methods for assessing risk
- Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth) including packet-level analysis techniques
- Knowledge and understanding of system and application security threats and vulnerabilities
- Knowledge and understanding of what constitutes a network attack and the relationship to both threats and vulnerabilities
- Knowledge and understanding of transmission methods and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly

\footnotesize{\textsuperscript{13} Ibid
\textsuperscript{14} Ibid
\textsuperscript{15} Adapted from Naval Air Systems Command, Standard Work Package for Cyber Developmental Testing & Evaluation (2016 July 28)}
F.3 Cybersecurity Roles and Responsibilities – RASCI

As discussed briefly in Section 3.2 of this guidebook, each Program Office should stand up a Cyber Working Group (CyWG) led by the CDT to ensure the accomplishment of the cybersecurity T&E Phase tasks. The CyWG is a cross-organizational and cross-functional group with potential for confusion about roles and responsibilities. One method to manage the roles and responsibilities for planning and conducting cybersecurity T&E is to build a RASCI (Responsible, Accountable, Supporting, Consulting, Informed) matrix listing the various personnel and their appropriate RASCI for each task, as appropriate. Figure F-1 is an example RASCI matrix that specifies some roles and responsibilities of those involved with planning and conducting cybersecurity T&E by cybersecurity T&E phase.

<table>
<thead>
<tr>
<th>Major Cybersecurity Tasks</th>
<th>R=Responsible, A=Accountable, S=Supporting, C=Consulting, I=Informed</th>
<th>Comments</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compile List of Cybersecurity and Resiliency Requirements</td>
<td>A S S C S C R S C S C C S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare for Cybersecurity T&amp;E Events</td>
<td>A S S C S S R R S S S C S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Cybersecurity T&amp;E Strategy</td>
<td>A S S C C C R R S S S C C I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the Cyber-Attack Surface</td>
<td>A S S C S C C R S S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze the Cyber-Attack Surface</td>
<td>A S S C S S C C R S S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document Analysis Results and Update Test Plans</td>
<td>A A C R S S S I I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare for Phase 3 and 4 Cybersecurity T&amp;E Events</td>
<td>A A R S S S I I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan CVI Test Activities</td>
<td>A S S R S S C C S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct CVI Events</td>
<td>A S S R S S C C S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document CVI Test Results</td>
<td>A S S R C C C I I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare for Phase 4 Cybersecurity T&amp;E events</td>
<td>A S S R S C C C S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Cyber Threat Assessment</td>
<td>A S S S S S R S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Kill Chain Analysis</td>
<td>A S S S S S C C R S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Adversarial DT&amp;E</td>
<td>A S S C C R S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct ACD</td>
<td>A S S S R S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document ACD Test Results</td>
<td>A I S I I I R I S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan CVPA</td>
<td>S S A R S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordinate with Cybersecurity Vulnerability Assessment Team</td>
<td>S A R S S S S I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute CVPA and Document Results</td>
<td>S S A A R S S S I</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure F-1. Example RASCI Table**

### F.3.1 RASCI Definitions

**R: Responsible**

Those who do the work to achieve the task. There is typically one role with a participation type of Responsible, although others can be delegated to assist in the work required (see Support).

**A: Accountable**

The approver or final approving authority; those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom Responsible is accountable. In other words, an Accountable must sign off (approve) on work that Responsible provides. There must be only one Accountable specified for each task or deliverable.
S: Supporting

Resources allocated to Responsible. Unlike Consulting, who may provide input to the task, Support will assist in completing the task.

C: Consulting

Those whose independent opinions and review are sought and with whom there is two-way communication.

I: Informed

People who are affected by the activity/decision and therefore need to be kept informed, but do not participate in performing the actual task. Informed needs to know of the decision or action.

F.4 Maintaining Cybersecurity T&E Proficiency

Acquisition programs and Services should examine their current and future cybersecurity T&E workforce needs, and identify and develop training resources to maintain and raise the level of technical competence of their cybersecurity test resources. Services should:16

- Understand specific and unique cybersecurity workforce needs
- Identify existing and future cybersecurity workforce development activities
- Coordinate with other Services and government agencies to broaden perspectives and share knowledge and experience by:
  - Participating in training or professional development exchanges
  - Observing test events not directly associated with the acquisition program
- Increase engagement with academia to expand and fill the cybersecurity T&E workforce pipeline
- Provide cybersecurity training for specific tester skills (hands-on and analytical skills)
- Create guidelines, tools, and other resources to develop, customize and deliver cybersecurity training and education materials

Cybersecurity T&E training requires a combination of formal classroom instruction including hands-on exercises along with on-the-job (OJT) and simulated job tasks experience to be the most effective. Training strategies include:

- Formal and informal classroom training –
  - Helps test teams stay up to date with new technologies
  - Supports non-traditional information technology specialties such as bus architectures
  - Teaches architecture analysis, reverse engineering principles, and other engineering principles useful during developmental testing
- Hands-on Training and On-the-Job Training
  - Sharing staff across multiple acquisition programs and Services
  - Cross-training staff between related test tasks (e.g., component testing versus integrated system testing)
  - Participating in hands-on activities such as simulated Red Team exercises and competitive activities such as Capture the Flag, or hackathons

16 Adapted from NIST Roadmap for Improving Critical Infrastructure Cybersecurity, Cybersecurity Workforce (February 12, 2014)
A variety of resources are available to identify formal classroom training environments:

- Defense Acquisition University
- NICCS Education and Training Catalog - https://niccs.us-cert.gov/training/\(^{17}\) - Hosted by DHS, the NICCS Training Catalog provides a robust listing of cybersecurity and cybersecurity-related training courses offered in the U.S. The Training Catalog contains over 3,000 courses
- Federal Virtual Training Environment (FedVTE) - Provides free online cybersecurity training to U.S. government employees, Federal contractors, and veterans
- Cybrary - https://www.cybrary.it/catalog/ - Provides free and fee-based cybersecurity training on a variety of popular topics

### F.5 Cybersecurity T&E Staffing in the TEMP

The TEMP should describe personnel resources needed to support the cybersecurity T&E test strategy including personnel required for cybersecurity analysis, testing and assessments. The TEMP should include a brief description of cybersecurity T&E roles and responsibilities. There should be a high-level summary of the personnel resources needed to execute cybersecurity testing. The cybersecurity T&E resources should be in alignment with the T&E budget exhibits (ACAT I Programs). These elements include funding, manpower for test conduct and support (e.g., cybersecurity teams, subject matter experts, additional testers, data collectors, trusted agents, etc.). cybersecurity T&E resources provided by the contractor must also be identified in either the development or production contract. For more information about TEMP requirements, refer to the Defense Acquisition Guidebook (DAG), Chapter 8.

### F.6 Cybersecurity T&E Organizations

For a current list of T&E organizations, CDTs should refer to DAG Chapter 8 (Section 2.2.3.2) which provides a list of T&E capability web links by DoD Component. For assistance identifying cybersecurity T&E expertise within or external to the T&E organizations, PMs should ask their T&E organizations, Service or Component T&E leadership, or OSD T&E.

Appendix G  Considerations for Software Assurance Testing

The purpose of this appendix is to ensure the CDT develops a software test strategy that addresses the security and functionality of the software, with an expectation of confidence derived from executing it. Software testing provides a risk-based level of assurance that (1) the software functions as intended, (2) known vulnerabilities are sufficiently mitigated, and (3) residual risk is consciously accepted.

This appendix assists the CDT by:

- Identifying test phases for software
- Identifying test methods and level of rigor applied to test strategy to achieve the desired level of software assurance
- Aligning software testing activities with the cybersecurity T&E phases
- Identifying key inputs for the development of the TEMP to ensure the software test strategy is properly planned, resourced, and scheduled and,
- Identifying contractual requirements that reflect the desired confidence needed to achieve an acceptable risk level within the RFPs.

Software testing helps discover vulnerabilities and produces evidence about the avoidance and removal of known vulnerabilities, underappreciated vulnerabilities (miscalculated, improperly assessed, etc) and unknown vulnerabilities. When the CDT employs software testing, uncertainty reduces, confidence increases (both positive and negative) about the software and the test results influence decisions about how to mitigate vulnerabilities that remain. Software testing activities are designed to demonstrate that validated requirements have been satisfied and evaluate the software’s functionality and security.

Test activities should align with the mission risk-based criteria used to evaluate the security of the acquisition program. Software supporting mission-critical functions often requires more rigorous testing to achieve the level of confidence for acceptable risks. Testing reduces mission risk by identifying underappreciated and unknown vulnerabilities that result from more rigorous and complex testing.

G.1  Understanding Software Functionality

A software stack is a group of software programs (e.g., applications, operating systems, virtual machines) that work together to produce results. A system includes computer hardware and software that works concurrently to create a complete platform (Figure G-1). For simplicity, this appendix uses an example of a generic representation of a computer hardware and software stack to demonstrate how coding/hardware flaws and test phases apply to the multiple layers.

G.2 Software Susceptibility

Coding flaws can lead to vulnerabilities across the entire software stack. The impact of triggering or exploiting vulnerabilities vary from component to component and acquisition program to acquisition program. For this reason, software testing to achieve a sufficient understanding of code behavior (or lack of) and forced behavior is imperative. Understanding how the code behaves in different circumstances require multiple test events focused on different software layers.

Once a vulnerability intentionally or unintentionally triggers within the stack, ripple effects may traverse various levels of the software stack as other systems software stacks. Figure G-2 demonstrates an attack path at the initial point of compromise to the system and the compromise of the attack. Although the entry was through an application, the software stack presents an opportunity for exposure at any level.
Considerations for Software Assurance Testing

**Applications** – Coding flaws at the application layer create security vulnerabilities that may be independent of the rest of the system stack or may enable exposures further down the stack.

**Operating System and Drivers** – Coding flaws at the operating system level have a broad impact on system security and reliability. Exploiting a vulnerability at the operating system layer may allow access to the API, kernel, device drivers, and multiple applications and data. Examples of malware that may exploit vulnerabilities include ransomware, trojan horses, and operating system rootkits.

**Virtual Machine Manager** – Because virtual machine managers control the abstractions and translations between virtual and hardware memory management, operating systems, networking, and other critical computer system components, coding flaws in the virtual machine manager level can expose or lead to many possible vulnerabilities or exploits of the whole system. An example of exploiting a vulnerability in the virtual machine manager is the installation of a virtual machine rootkit.

**Firmware** – Coding flaws in the firmware layer may expose vulnerabilities at the hardware level or upper software layers and highlights hardware-software co-dependencies. Exploiting firmware vulnerabilities may allow control of memory allocation, processing, or hardware elements such as the BIOS/UEFI, memory devices, cryptographic key storage, etc. An example of exploiting a vulnerability in firmware is the installation of BIOS rootkits.

**Hardware** – Flaws in the electronic hardware (analog circuits or digital logic design) layer may expose vulnerabilities in the system that are not detectable or mitigated by software layers. The hardware layer may expose operational security flaws in the upper layers as it has visibility of all software requests for hardware resources. An example of exploiting a vulnerability at the hardware level involves compromising a hardware component in the supply chain that enables a future cyber-attack causing system failure, or a direct memory access exploit.

Figure G-3, gives a real-world example of a common Windows software stack. In general, the software layers only have access to information provided by the API and do not have visibility into the layers below them, meaning the application layer (top) may not be able to detect vulnerabilities in the hardware layer (bottom layer).
Supply chain exposures significantly affect the security of software. For example, an adversary may deliberately compromise software, firmware, and microelectronics while in the supply chain with the intent to exploit future systems that results in system failures. Undiscovered and unappreciated weaknesses, defects, or flaws in software provide the foundation for threat actors to defeat fielded systems through cyber-attacks and provides for intentional, accidental, or erroneous actions to produce adverse effects.

G.3 Understanding Test Phases

Software testing occurs in various phases of software development. Following the development lifecycle of the software, the test phases include unit test, integration test, system test, and integrity test as shown in Figure G-4. An important consideration during the testing phases is ensuring that the tests are designed to find anomalies at the appropriate level. The types of tests performed vary with each testing phase, although testers can apply almost any of the techniques at any phase. Test phases can translate to the depth, breadth, and confidence associated with software test methods. Testing may vary within and across components depending on the level of rigor needed to reach confidence in the system’s security.

The software testing identified for an acquisition program is a function of the consequence of loss. Criticality and risk acceptance determine consequence. Components may have various levels of acceptable risk and different software stacks. Designing a software test strategy can be accomplished once there is an understanding of the test phases needed as it relates to the component’s software stack.


Considerations for Software Assurance Testing
Figure G-4. Software Testing Strategy

Unit test – Software testing conducted on the units or software modules in each layer. Unit describes the smallest testable element since different layers have various constructs. For example, the application layer can be broken down into modules, and the operating system level can be broken down into services. Unit testing is the best opportunity to perform failure mode, and fault insertion testing where the functionality contained in the unit must respond correctly and safely. Unit testing consists of multiple static, dynamic, and hybrid testing methods. Table G-3 identifies examples of unit test methodologies.

Integration test – Software testing in which the individual units or software modules are combined and tested as a group. Integration testing occurs within the application layer and between the software stack layers. Integration requires both horizontal and vertical testing within the stack and provides confidence about the behaviors, interactions, and outcomes produced across layers. Integration testing also examines if establishing an interface amongst modules compromises functionality and integrity of the relationship and dependencies between units of code. Incremental integration testing more readily identifies errors then conducting system testing right away.

It is important to test and observe interactions between critical software modules and to study the system response. In some cases, a potentially minor flaw/vulnerability identified in Unit Testing or Code review of a single module can have a significant impact at the system level. It is important to trace and document the cascading effects of small software flaws at the system impact level. Many times, these are second and third order cascading failures a novice test engineer may not consider in his or her first order system test designs. Integration testing consists of multiple static, dynamic, and hybrid testing methods. Table G-3 identifies examples of integration test methodologies.

System test – Software testing conducted on a complete, integrated system. System testing confirms behaviors of interfaces based on insights and knowledge gained from the previous unit and integration

Considerations for Software Assurance Testing

testing. The system test is the maximized integration test of the entire software stack, coupled with the environment and user.

**Integrity test** – Software testing that establishes a known integrity baseline for assured delivery. The baseline is used to ensure the final software version has maintained integrity through delivery and implementation. It is often coupled with chain-of-custody operations and cryptographic test techniques, to include digitally signed software packages.

### G.4 Software Implementation Options

Program Managers have the responsibility to deliver functional, resilient software components as part of the system. There are three general options for software implementation - software can be developed, reused, or acquired off the shelf. Each software implementation has advantages and disadvantages. The trade space between the software options considers threats to the acquisition program, the required testing rigor needed to provide confidence in the solution, and allowable testing.

**Developed** – This includes software a contractor develops for an acquisition program. The PM must communicate the level of rigor in the software development plan. The contractor must understand the testing rigor the software requires before beginning software development. The RFP, or a controlled source document referenced by the RFP, must include details of design, processes, methods, and tools utilized for testing.

To ensure operational security, consider instituting a controlled process of exchanging details on test requirements. For example, if an adversary were to know static analysis using Fortify is the only test requirement, then the adversary could use that knowledge to develop an attack path undiscovered by Fortify.

Ideally, contractor developed software testing is with a government representative observing to decrease duplicative acceptance testing. If the contractor conducts the software testing without a government representative present, testing rigor follows the risk acceptance level of the PM. Government acceptance testing evaluates compliance with requirements during subsequent testing.

**Reuse** – Reused software use previous unit test results. The test strategy considers prior unit test results, and plans for integration tests and systems tests. Reuse may include previous testing results, which may then only require a simple regression testing or updated testing that accounts for new threats.

**Off the shelf** – There are two types of off the shelf software: commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS).

- Software testing of COTS has limits due to its development external to the acquisition program. Limits increase uncertainty regarding its vulnerability and maximum achievable assurance. Integration and systems testing is critical. COTS software used on a mission-critical system should have a high level of rigor applied to testing.

- Software testing of GOTS includes unit, integration, and system testing and adhere to the required rigor.
G.5 Cybersecurity T&E Phases

Cybersecurity T&E phases include analysis and planning for software testing. Figure G-5 shows the distribution of software testing activities across the cybersecurity T&E process.

![Software Testing Schedule Diagram]

**Figure G-5. Software Testing Schedule**

G.5.1 Phase 1 – Understand the Cybersecurity Requirements

Phase 1 is fundamental to scoping test activities, to include test types, timelines, resources, and identification of specified and derived requirements. Implied software test requirements derive from the PPP countermeasures, the Assured Software Development (ASD) STIG, the TSN analysis, and the SEP. As an example, while the PPP calls for implementing developmental and operational countermeasures for software vulnerabilities during the software development process, requirements may not have considered evolving threats to the new system (derived from open source intelligence and other sources). Table G-1 shows a list of software testing requirements that should be considered for testing. Testers must revisit requirements as evolving, and new threat information emerges that could result in operational impact. The timing and scope of tests must target the test rigor corresponding with risk acceptance.

**Table G-1. Cybersecurity Software Test Requirements**

<table>
<thead>
<tr>
<th>Source</th>
<th>Notionally Implied Cybersecurity SW Test Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP</td>
<td>Test requirements confirm:</td>
</tr>
<tr>
<td></td>
<td>• Mitigation of CVEs</td>
</tr>
<tr>
<td></td>
<td>• Mitigation of common Attack pattern enumeration and classification</td>
</tr>
<tr>
<td></td>
<td>• Mitigation of common weakness enumeration</td>
</tr>
<tr>
<td></td>
<td>• Effectiveness of fault isolation</td>
</tr>
<tr>
<td></td>
<td>• Effectiveness of least privilege</td>
</tr>
<tr>
<td></td>
<td>• Achievement of system element isolation</td>
</tr>
<tr>
<td></td>
<td>• Input checking and validation measures</td>
</tr>
<tr>
<td>TSN</td>
<td>Includes software security focused test requirements in development contracts. Describes contractor software testing activities</td>
</tr>
<tr>
<td>STIGs</td>
<td>Confirm compliance with ASD STIG</td>
</tr>
</tbody>
</table>
### Considerations for Software Assurance Testing

#### SEP
- Scheduling requirements for software releases
- Scheduling requirements for hardware and software integration events that are informed by security concerns
- Scheduling and integration requirements for linkage between hardware and software upgrade programs within the family of systems or system of systems

#### VOLT report
- Test rigor required based on program threat assessment

#### PPP/Criticality Analysis
- Test rigor required based on mission criticality and impacts from loss of functionality

---

#### G.5.2 Phase 2 – Characterize the Cyber-Attack Surface

The cybersecurity T&E team characterizes the software to understand the attack surface and dependencies. At a minimum, inspecting/analyzing the design for known security issues using sources from Table G-2 suggests resources that help identify the software attack surface.

**Table G-2. Characterization Sources**

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
</table>
| CAPEC                | Comprehensive dictionary and classification of know attacks.  
21 capec.mitre.org  |
| CWE                  | List of common software security weaknesses.  
22 cwe.mitre.org  |
| CVE                  | List of common identifiers for publicly known cybersecurity vulnerabilities.  
23 cve.mitre.org  |
| OWASP Top 10         | Awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications from Open Web Application Security Project (OWASP).  
| MITRE ATT&CK model   | Curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s life cycle and the platforms they are known to target. MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.  
25 https://attack.mitre.org/wiki/Main_Page  |
| Robust parameter design | Experimental design used to exploit the interaction between control and uncontrollable noise variables.  |
| Subject Matter Expert on system security | Knowledge of system security to include system threats and vulnerabilities.  |
| Subject Matter Expert on system mission | Knowledge of mission impact due to security effects on various components.  |

---

#### G.5.3 Phase 3 – Cooperative Vulnerability Identification

CVI testing includes scale and scope required to demonstrate the level of confidence needed for the software. Common techniques include categories of static, dynamic, and hybrid static/dynamic. The IDA publication *State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation* includes resources. For example:

1. **Source**: Comprehensive dictionary and classification of know attacks.
   - [capec.mitre.org](capec.mitre.org)
2. **Source**: List of common software security weaknesses.
   - [cwe.mitre.org](cwe.mitre.org)
3. **Source**: List of common identifiers for publicly known cybersecurity vulnerabilities.
   - [cve.mitre.org](cve.mitre.org)
4. **Source**: Awareness document for web application security.
5. **Source**: Curated knowledge base and model for cyber adversary behavior.
   - [https://attack.mitre.org/wiki/Main_Page](https://attack.mitre.org/wiki/Main_Page)

---

*Considerations for Software Assurance Testing*
2016\textsuperscript{26} details various tools and techniques, manual and automatic, for the categories of tests as seen in Table G-3. The SOAR document defines the categories as:

- **Static analysis**: Examines the system/software without executing it, including examining source code, bytecode, and binaries.
- **Dynamic analysis**: Examines the system/software by executing it, giving it specific inputs, and examining results and outputs.
- **Hybrid analysis**: Tightly integrates static and dynamic analysis approaches. For example, test coverage analyzers use dynamic analysis to run tests and then use static analysis to determine which parts of the software had no tests. This grouping is used only if static and dynamic analyses are tightly integrated; a tool or technology type that is primarily static or primarily dynamic is put in those groupings instead.

The SOAR document identifies tools and techniques, from the different categories, which assess how well they perform to meet the following ten high-level technical objectives:

- Provide design and code quality
- Counter known CVEs
- Ensure authentication and access control
- Counter unintentional "like" weaknesses
- Counter unintentional "like" malicious logic
- Provide antitamper and ensure transparency
- Counter development tool inserted weakness
- Provide secure delivery
- Provide secure configuration
- Excessive power consumption

It is imperative to understand that one tool does not meet all the SOAR’s listed objectives. Each acquisition program has different technical objectives for software testing. Cybersecurity testers should understand their selected tools’ capabilities and limitations. Appendix E of the SOAR for Software Vulnerability Detection, Test, and Evaluation (revision 10) Matrix\textsuperscript{27}, provides an excellent example of cross-referencing testing objectives with the capabilities of the tools and techniques listed in Table G-3.

The testing methods identified in Table G-3, support findings at various levels of the software stack. One tool or method does not discover all vulnerabilities. When developing a test strategy, it is important to understand what is and is not being tested to understand residual risk. Each acquisition program must determine the sufficient level of rigor needed based on the threats and criticality of the system.

<table>
<thead>
<tr>
<th>Category</th>
<th>Tool/Techniques</th>
</tr>
</thead>
</table>
| **Static Analysis** | • Attack modeling  
                     | • Warning flags  
                     | • Source code quality analyzer  
                     | • Source code weakness analyzer  
                     | • Context-configured source code weakness analyzer  
                     | • Source code knowledge extractor for arch/design coding standards – Extract design, architecture, mission layer, to aid analysis |

\textsuperscript{26} Institute for Defense Analysis. *State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation* 2016.

\textsuperscript{27} Institute for Defense Analysis. *State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation (revision 10) Matrix*
<table>
<thead>
<tr>
<th>Category</th>
<th>Tool/Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Requirements-configured source code knowledge extractor – Extract design, architecture, mission</td>
</tr>
<tr>
<td></td>
<td>layer, to aid analysis</td>
</tr>
<tr>
<td></td>
<td>• Traditional virus/spyware scanner</td>
</tr>
<tr>
<td></td>
<td>• Binary/bytecode quality analysis</td>
</tr>
<tr>
<td></td>
<td>• Bytecode weakness analysis (including disassembler + source code weakness analysis)</td>
</tr>
<tr>
<td></td>
<td>• Binary weakness analysis - including disassembler + source code weakness analysis</td>
</tr>
<tr>
<td></td>
<td>• Inter-application flow analysis</td>
</tr>
<tr>
<td></td>
<td>• Binary/bytecode simple extractor – strings, ELF readers, etc.</td>
</tr>
<tr>
<td></td>
<td>• Compare binary/bytecode to application permission manifest</td>
</tr>
<tr>
<td></td>
<td>• Obfuscated code detection</td>
</tr>
<tr>
<td></td>
<td>• Binary/bytecode disassembler - then use manual analysis of vulnerabilities &amp; anomalies</td>
</tr>
<tr>
<td></td>
<td>• Focused manual spot check - Focused manual analysis of source</td>
</tr>
<tr>
<td></td>
<td>• Manual source code review (not inspections)</td>
</tr>
<tr>
<td></td>
<td>• Inspection (IEEE 1028 standard) (can apply to requirements, design, source code, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Generated code inspection</td>
</tr>
<tr>
<td></td>
<td>• Safer languages</td>
</tr>
<tr>
<td></td>
<td>• Secured library selection</td>
</tr>
<tr>
<td></td>
<td>• Secured OS</td>
</tr>
<tr>
<td></td>
<td>• Origin analysis</td>
</tr>
<tr>
<td></td>
<td>• Digital signature verification</td>
</tr>
<tr>
<td></td>
<td>• Configuration Checker</td>
</tr>
<tr>
<td></td>
<td>• Permission manifest analysis</td>
</tr>
<tr>
<td></td>
<td>• Development/sustainment version control</td>
</tr>
<tr>
<td></td>
<td>• Obfuscator</td>
</tr>
<tr>
<td></td>
<td>• Rebuild &amp; compare</td>
</tr>
<tr>
<td>Dynamic Analysis</td>
<td>• Network scanner - id (sub)systems &amp; ports</td>
</tr>
<tr>
<td></td>
<td>• Network sniffer</td>
</tr>
<tr>
<td></td>
<td>• Network vulnerability scanner – scan for already-known vulnerabilities for specific products</td>
</tr>
<tr>
<td></td>
<td>• Host-based vulnerability scanners – Examine configuration for flaws, verifying that audit mechanisms</td>
</tr>
<tr>
<td></td>
<td>work, ensure host configuration meets certain predefined criteria</td>
</tr>
<tr>
<td></td>
<td>• Host application interface scanner</td>
</tr>
<tr>
<td></td>
<td>• Web application scanner</td>
</tr>
<tr>
<td></td>
<td>• Web services scanner</td>
</tr>
<tr>
<td></td>
<td>• Database scanners</td>
</tr>
<tr>
<td></td>
<td>• Fuzz tester</td>
</tr>
<tr>
<td></td>
<td>• Framework-based fuzzer</td>
</tr>
<tr>
<td></td>
<td>• Negative testing – include tests that are supposed to fail due to security mechanisms properly</td>
</tr>
<tr>
<td></td>
<td>working</td>
</tr>
<tr>
<td></td>
<td>• Digital forensics</td>
</tr>
<tr>
<td></td>
<td>• Intrusion Detection Systems/Intrusion Prevention Systems</td>
</tr>
<tr>
<td></td>
<td>• Automated monitored execution</td>
</tr>
<tr>
<td></td>
<td>• Forced path execution</td>
</tr>
<tr>
<td></td>
<td>• Firewall (network &amp; web application)</td>
</tr>
<tr>
<td></td>
<td>• Man-in-the-middle attack tool</td>
</tr>
<tr>
<td></td>
<td>• Debugger</td>
</tr>
<tr>
<td></td>
<td>• Fault injection – source code</td>
</tr>
<tr>
<td></td>
<td>• Fault injection – binary</td>
</tr>
<tr>
<td></td>
<td>• Logging systems</td>
</tr>
<tr>
<td></td>
<td>• Security Information and Event Management (SIEM)</td>
</tr>
<tr>
<td>Hybrid Static/Dynamic Analysis</td>
<td>• Test coverage analyzer – statement or branch coverage</td>
</tr>
<tr>
<td></td>
<td>• Hardening tools/scripts</td>
</tr>
<tr>
<td></td>
<td>• Execute and compare with application manifest</td>
</tr>
<tr>
<td></td>
<td>• Track sensitive data</td>
</tr>
<tr>
<td></td>
<td>• Coverage-guided fuzz tester</td>
</tr>
<tr>
<td></td>
<td>• Probe-based attack with tracked flow</td>
</tr>
<tr>
<td></td>
<td>• Track data and control flow</td>
</tr>
</tbody>
</table>

**Test Rigor.** Military Standard 882 E defines the level of rigor as “a specification of the depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software functions perform as required.” Software testing methods used to
achieve safety can also be leveraged to achieve cybersecurity. Although safety and cybersecurity are different, the definition can be applied to cybersecurity testing as seen in Figure G-6. This figure visualizes the entire software system view to help demonstrate the level of rigor possible for software testing. The figure demonstrates the depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence in cybersecurity. Figure G-6 shows that unit, integration and system tests may include all three categories of analysis. For example, manual source code review, a static analysis method, can be conducted on a unit, multiple units integrated together, or on the entire system from any layer of the software stack.

![Figure G-6. Testing Rigor](image)

**G.5.4 Phase 4 – Adversarial Cybersecurity DT&E**

Phase 4 of software testing uses penetration testing to identify software vulnerabilities not previously identified at the software system phase. The test conducts an adversarial assessment. The intent is to circumvent software security functions and by doing so identify unknown and underappreciated vulnerabilities and to confirm known vulnerabilities have been sufficiently mitigated.

**G.5.5 Phase 5 – Cooperative Vulnerability Penetration Assessment**

The purpose of the CVPA phase is to provide a comprehensive characterization of the cybersecurity status of a system in a fully operational context and provide system vulnerability data to support adversarial testing. The CVPA occurs either after previously identified software vulnerabilities found in the CVI and ACD have been resolved or with test plan documented mitigations.

In OT, software examination is included in the context of the acquisition program system, not just the software system of the component. DT&E cybersecurity T&E phases cannot duplicate every nuance of the operational environment, nor can it duplicate every possible combination of events. Based on knowledge of threats and the software design, test engineers can develop procedures to test software paths specifically for security events. OT&E should include developing tests that examine the security of the software in the context of its operational environment and operational interactions.

Considerations for Software Assurance Testing
G.5.6 Phase 6 – Adversarial Assessment

The Adversarial Assessment phase assesses the ability of the system to support its missions while withstanding validated and representative threat activity as documented in the VOLT report.

In addition to assessing the effect on mission execution, the OTA evaluates the ability of the system, tiered defenses, and defenders to protect the system, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity.

G.6 Cybersecurity Testing for Software Reliability

The purpose of software reliability (SR) testing is to determine product reliability and determine whether the software meets reliability requirements. SR testing exercises the software application so that failures are discovered and removed before the system is deployed. SR requires analysis techniques with a clear understanding of the characteristics of potential software failures.

Software security shares many of the same challenges as software quality and reliability. As an example, many of the 900 CWEs that have been identified can be associated with poor quality coding, which reduces the software’s reliability and increases the potential for system exploitation by cyber adversaries. Security and reliability of operational software cannot be absolutely assured because software weaknesses may not appear until certain conditions, such as an external attack, cause a failure. Having no occurrences of reliability or security failures in operational software does not guarantee that the software is reliable or secure because there is no way of establishing that all defects/vulnerabilities have been removed. To increase the reliability of the software, SR testing should be supplemented by incorporating cybersecurity analysis using the CWE list, RMF security controls, network modeling, and operational scenarios used to define the attack surface, CTT exercises, static and dynamic analysis can improve the probability of failure-free software operations.

The framework to incorporate cybersecurity testing into reliability testing comprises the evaluation of hardware, software, network architecture and performance, information security, resilience and vulnerability, as a comprehensive reliability assessment of an entire system. Figure G-7 shows cybersecurity reliability modeled using known network attacks, system vulnerabilities and system components. Vulnerability reliability is tested and evaluated based on complex network theory. Resilience and elasticity reliability uses profile testing (scenarios) to observe the ability of a system to reconfigure and adapt to change (elasticity) and the ability of the system to adjust and sustain under expected and unexpected conditions (resilience). This approach requires more maturity, but the models suggested for each of the cyber reliability steps are often practiced in cybersecurity community.

28 Software Engineering Institute, Predicting Software Assurance Using Quality and Reliability Measures, (December 2014)
29 Ibid
30 IEEE, Strategy for reliability testing and evaluation of cyber physical systems (December 2015)
When there is a software reliability requirement for the system, the CDT should consider incorporating the following cybersecurity test activities into SR test activities:

- **Functional (Feature) Testing.** Cyber compromises can adversely affect the functionality of a software system. Using the defined RMF controls performed in the cybersecurity T&E analysis and planning, outline the testing features required for test and ensure that during the test that any of the CWE encountered are documented and corrected. Functional testing of the interactions between features can further identify any CWE issues. Static analysis on the software system under test should be conducted prior to this test. Fuzz testing to test input validation may also be an option to ensure that the feature tested cannot be exploited by incorrect inputs. Feature testing can be conducted during Phase 3 CVI activities.

- **Regression Testing.** Once a software modification has been completed, the integrity of the software is at risk because the new software may introduce or expose undetected vulnerabilities in the unchanged software. Repeating relevant cybersecurity tests performed during Feature testing will improve the probability of failure-free software.

- **Scenario Testing.** This type of testing can leverage or enhance CTTs. Incorporating CTTs to help define realistic scenarios that can be run during Scenario testing. Using Cyber Ranges or simulating the attack environment during the Adversarial Cybersecurity DT&E will contribute to the SR of the software system.

Incorporated cybersecurity test practices into SR testing and leveraging the results of the cybersecurity T&E phases may improve both SR and security of the operational system’s software.

### G.7 Cybersecurity Software Testing in RFPs

TSN Analysis, Appendix A, Part 2, June 2014 lists a set of software development and testing items that may assist PMs in reviewing their software development contracts for software testing practices. The list below provides an example of contract software testing items from the TSN Analysis:

1. **SOW requires the contractor to establish secure design and coding standards for critical function components developmental software (and verifies through inspection or code analysis)**
   - The contractor should consider CWE, and Software Engineering Institute Top 10 secure coding practices and other sources when defining the standards.

2. **SOW requires the contractor to use static analysis tools to identify violations of the secure design and coding standards for critical function components.**
3. SOW requires design and code inspections to identify violations of secure design and coding standards for critical function components.
4. SOW requires the mitigation of common software vulnerabilities. Derive from:
   a. CWE
   b. CVE
   c. CAPEC
5. SOW requires penetration testing based on malicious insertion and other security abuse cases.
6. SOW requires specific code test-coverage metrics to ensure adequate testing of critical function components.
7. SOW requires regression tests following changes to critical function code.
8. System Requirements Document require software fault detection, fault isolation, and tracking (or logging) of faults and cybersecurity attacks.
9. SOW require critical function developmental software to be designed with least privilege to limit the number, size, and privileges of system elements.
10. System Requirements Document requires a separation kernel or other isolation techniques for Level I critical function components to control communications between Level I critical functions and other critical and noncritical functions.
11. System Requirements Document requires a software load key to encrypt and scramble software to reduce the likelihood of reverse engineering.
12. Systems Requirements Document requires parameter checking and validation for the interfaces to critical function components.
13. SOW requires that access to the development environment is controlled with limited authorities (least privilege), and does it ensure logging and tracing of all code changes to specific individuals.
14. SOW requires commercial off-the-shelf (COTS) product updates to be applied and tested within a specified period after release from the original equipment manufacturer or another software provider.

G.8 Cybersecurity Software Testing in the TEMP

The TEMP must reflect software testing activities and include a schedule of assessments (TEMP Part II), resources required for software assessments (TEMP Part IV), and describe the software T&E tests that occurs in phases 1 through 6 (TEMP Part III). The CDT should review the test objectives for software testing and document in the TEMP and detailed test plans:

- Software phases to be tested (unit, integration, and system)
- Order in which the integration software testing must be designed, developed, and assessed
- Depth and breadth of testing as it relates to the software stack
- Requirements for, and timing of the ASD STIG compliance testing
- Consider the software testing rigor for inclusion in the Development Request for Proposal (RFP) for design, development, and assessment by the contractor
- Required software performance technical objectives with accommodating testing technique

The T&E Strategy documented in the TEMP must explain how the execution of software test activities provide data for evaluations, and how those evaluations provide decision makers with essential information.
information about the cybersecurity of the software. It must explain how test organizations carry out the software test activities.

As part of the OT Evaluation Framework, the TEMP must include measures for software as part of operational test plans to include procedures for software changes with upgrades, updates, and pre-planned (or unplanned) product enhancements.

G.9 Joint Federated Assurance Center

The Joint Federated Assurance Center (JFAC) is a federation of DoD organizations that promotes software and hardware assurance by providing expertise and support to defense acquisition programs and supporting activities. Through JFAC Service Providers, acquisition programs may obtain life cycle software security engineering services, including:

- Subject Matter Expert (SME) support during lifecycle software security engineering activities (e.g. software security design, criticality analysis, supply chain risk management, milestone reviews, sustainment support).
- Identification of applicable Software Assurance requirements from policy, standards, instructions, and guidance.
- Assistance with Software Assurance contract language.
- Assistance with Software Assurance metrics.
- Evaluation and Recommendation of appropriate Software Assurance tools for developer use.
- Integration of Software Assurance tools into the software development, test, & sustainment environments.
- Software Assurance training for management and software engineering staff.

More information about JFAC resources may be found at https://jfac.navy.mil/#

G.10 Additional References

- Trusted Systems and Networks (TSN) Analysis, Developed by DASD (SE) and DoD CIO (June 2014).
<table>
<thead>
<tr>
<th>Appendix X1</th>
<th>Considerations for Cybersecurity Requirements and Measures for DT&amp;E (FOUO Document)</th>
</tr>
</thead>
</table>
For Official Use Only (FOUO) appendices are accessible to government and authorized contractor personnel at the following link:  
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx |

<table>
<thead>
<tr>
<th>Appendix X2</th>
<th>Appendix X2  Cyber Threat Assessment for Cybersecurity T&amp;E (FOUO Document)</th>
</tr>
</thead>
</table>
For Official Use Only (FOUO) appendices are accessible to government and authorized contractor personnel at the following link:  
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx |

<table>
<thead>
<tr>
<th>Appendix X3</th>
<th>Mission-Based Cybersecurity Risk Assessments (FOUO Document)</th>
</tr>
</thead>
</table>
For Official Use Only (FOUO) appendices are accessible to government and authorized contractor personnel at the following link:  
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx |

<table>
<thead>
<tr>
<th>Appendix X4</th>
<th>Cybersecurity Test Infrastructure and Environment Planning (FOUO Document)</th>
</tr>
</thead>
</table>
For Official Use Only (FOUO) appendices are accessible to government and authorized contractor personnel at the following link:  
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx |

<table>
<thead>
<tr>
<th>Appendix X5</th>
<th>Cybersecurity Test Considerations for Non-IP Systems (FOUO Document)</th>
</tr>
</thead>
</table>
For Official Use Only (FOUO) appendices are accessible to government and authorized contractor personnel at the following link:  
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx |