

Department of Defense

Cybersecurity Test and Evaluation Guidebook

February 10, 2020

Version 2.0, Change 1



CLEARED
FOR OPEN PUBLICATION
FEB 06 2020
CASE # 20-S-0618
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Questions and issues regarding the content and format of this document, please email
guidebookfeedback@mitre.org



For technical issues and questions regarding Cybersecurity Developmental Test and Evaluation,
please email

osd.pentagon.ousd-re.mbx.communications@mail.mil

Office of the Under Secretary of Defense, Research and Engineering, Advanced Capabilities,
Developmental Test and Evaluation and Prototyping (<https://ac.cto.mil/dtep/>)



For technical issues and questions regarding Cybersecurity Operational Test and Evaluation,
please email

Mr. David Aland (david.j.aland.civ@mail.mil)

Office of the Director, Operational Test and Evaluation (<https://www.dote.osd.mil/>)

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 Fiscal Year 2016 National Defense Authorization Act (NDAA) Section 804..... 3

2.3 Business Systems Requirements and Acquisition, DoDI 5000.75 4

2.4 Cybersecurity, DoDI 8500.01 4

2.5 Cybersecurity Activities Support to DoD Information Network Operations (DODIN), DoDI 8530.01 6

2.6 Joint Requirements Guidance..... 6

2.7 DOT&E Cybersecurity Procedures Memoranda..... 7

3 Cybersecurity Test and Evaluation Overview 8

3.1 Cybersecurity T&E Phases Overview 8

3.2 Cybersecurity Working Group 11

3.3 Cybersecurity Threat Assessments..... 12

3.4 DT&E and SE Collaboration..... 12

3.5 Early Tester/Analyst Involvement..... 14

3.6 Mission-Based Cyber Risk Assessments 15

3.7 Role of Cybersecurity Developmental Testing 15

3.8 Integrated Testing..... 20

4 Phase 1: Understand Cybersecurity Requirements (and Plan for T&E)..... 23

4.1 Schedule 23

4.2 Inputs 24

4.3 Tasks 25

4.4 Phase 1 Data Requirements..... 29

5 Phase 2: Characterize the Cyber-Attack Surface 31

5.1 Schedule 31

5.2 Inputs 32

5.3 Tasks 33

5.4 Phase 2 Data Requirements..... 42

6 Phase 3: Cooperative Vulnerability Identification..... 44

6.1	Schedule	45
6.2	Inputs	45
6.3	Tasks	46
6.4	Phase 3 Data Requirements.....	56
7	Phase 4: Adversarial Cybersecurity DT&E.....	58
7.1	Schedule	59
7.2	Inputs	59
7.3	Tasks	59
7.4	Phase 4 Data Requirements.....	65
8	Phase 5: Cooperative Vulnerability and Penetration Assessment	66
8.1	Schedule	66
8.2	Inputs	67
8.3	Tasks	67
8.4	Outputs	69
9	Phase 6: Adversarial Assessment.....	70
9.1	Schedule	70
9.2	Inputs	71
9.3	Tasks	71
9.4	Outputs	72
10	Acronyms and Glossary of Terms	73
10.1	Acronyms	73
10.2	Cybersecurity T&E Glossary of Terms.....	77
11	References	83
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 Developmental Evaluation Framework (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	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 6

Figure 3-1. Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle 8

Figure 3-2. Cybersecurity T&E Phases Are Iterative 11

Figure 3-3. Interaction of SE and T&E Cybersecurity Activities 13

Figure 3-4. Cybersecurity Testing Requirement Venn Diagram 16

Figure 3-5. Interaction of RMF and T&E Cybersecurity Activities 17

Figure 4-1. Phase 1: Understand Cybersecurity Requirements Activities 23

Figure 4-2. Phase 1 Iteration 24

Figure 5-1. Phase 2: Characterize the Cyber-Attack Surface Activities 31

Figure 5-2. Phase 2 Iteration 32

Figure 5-3. Example Mission Decomposition and Criticality Analysis 36

Figure 5-4. Example Cyber-Attack Surface System Diagram 37

Figure 5-5. Cyber Kill Chain 39

Figure 5-6. Example Attack Surface Analysis 40

Figure 5-7. Threat Vignette Illustration 41

Figure 6-1. Phase 3. Cooperative Vulnerability Identification Activities 44

Figure 6-2. Phase 3 Testing Process 44

Figure 6-3. Phase 3 Iteration 45

Figure 7-1. Phase 4: Adversarial Cybersecurity DT&E Activities 58

Figure 8-1. Phase 5: Cooperative Vulnerability and Penetration Assessment Activities 66

Figure 9-1. Phase 6: Adversarial Assessment Activities Schedule 70

Figure C-1. Adaptive Acquisition Framework (AAF) Pathways C-1

Figure C-2. Tailored Cybersecurity T&E 6 Phase Process C-2

Figure C-3. T&E During Agile Software Development C-6

Figure C-4. The Sec in DevSecOps C-7

Figure C-5. Cybersecurity T&E Phases Mapped to the BCAC Process C-11

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 E-4. Cyber Portion of the DEF for Agile Development Process E-8

Figure F-1. Vulnerability Analyst Proficiency and Maturity Levels F-5

Figure F-2. Example RASCI Table F-8

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 3-1: SS KPP Pillars and Cyber Survivability Attributes (CSAs)..... 20

Table 4-1. Cybersecurity and Resilience Requirements and Testing Factors to Consider 25

Table 5-1. Mobile Navigation System (Notional) Attack Surface List..... 34

Table 6-1. Example Program Test Objectives, Technical Test Objectives and Metrics..... 48

Table 6-2. Example Test Activities..... 50

Table 6-3. Cybersecurity DT&E Activities and Cybersecurity Test Facilities..... 54

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 C-1. BCAC Acquisition Decisions Informed by Cybersecurity T&E C-12

Table G-1. Cybersecurity Software Test Requirements G-7

Table G-2. Characterization Sources G-8

Table G-3. Sample Test Methods G-10

DoDI Cybersecurity T&E Guidebook v2 Change 1 Significant Changes

Cybersecurity Requirements – Cybersecurity standards, operational resilience and system cyber survivability requirement test considerations were added throughout the document. Chapter 3, section 3.7 explains the cybersecurity requirements associated with the Risk Management Framework (RMF), Department of Defense Instruction (DoDI) 8500.01, and the Cyber Survivability Endorsement Implementation Guide (CSE IG) to include the Cyber Survivability Risk Posture (CSRP). Chapters 4, 5, 6, and 7 explain how these requirements are addressed in cybersecurity Test and Evaluation (T&E) Phases 1, 2, 3, 4.

Testing Defensive Cyber Operations (DCO) – Testing guidance was added throughout the Guidebook to address analyzing and testing a system’s DCO defensive measures. This guidance adheres to DoDI 8530.01.

Contractor testing and integrated contractor and government test activities – Language was added to each phase that addresses early (during development) contractor test activities, contractor test activities for rapid prototype and rapid fielding programs, and contractor remediation of discovered vulnerabilities.

Appendix B – Contract language considerations were added to address software development practices, development environments, software assurance testing. Suggested language was also added to address contractor-government integrated cybersecurity testing during system development, contractor testing during prototype and rapid fielding development, and contractor remediation of system vulnerabilities discovered during testing.

Appendix C – The current six Phase process is closely coupled with DoDI 5000.02 acquisition phases and milestones. To provide guidance for tailoring the phases, Appendix C adds a new six Phase diagram that is decoupled from any specific acquisition model. Appendix C also includes the following changes:

- Agile and DevSecOps: A new section was added to discuss tailoring phases for Agile software development and DevSecOps for contractor and government testers.
- Middle Tier Acquisitions (MTA): A new section was added to discuss tailoring of Rapid Prototyping and Rapid Fielding for MTA programs.

Appendix E: The cyber portion of the Developmental Evaluation Framework (DEF) now includes an example of a DEF tailored for programs using Agile development methods.

Appendix F: The DoD Cybersecurity Developmental Test Cross-Service working group (XSWG) recently recommended a set of Development Test Cyber Vulnerability Analysis (VA) Standards. Appendix F was updated to include a summary of the VA standards. The VA standards recommend organizational level and analyst level standards. The organizational standards describe recommended administrative capabilities to support test events, staff cyber VA personnel, and develop and retain Cyber DT VA workforce. The analyst level standards include a set of Knowledge, Skills and Abilities (KSAs) and a progression of knowledge for Cybersecurity VAs.

Additional changes and corrections are listed in the table below.

Record of Changes		
Version	Effective Date	Summary
1.0	1 July 2015	Initial release, version 1.0
2.0	25 April 2018	Initial release, version 2.0
2.0 Change 1 Review Draft	4 November 2019	New section 2.2: Section 804/MTA policy, new section 2.5 DoDI 8530.01
		Chapter 3: Updated figure 3-1, 3-3, 3-5, added new figure 3-4, updated sections 3.1, 3.2, 3.3, 3.4, 3.5, 3.8; added new section 3.7: operational

		resilience and cyber survivability testing; updated figure 3-3
		Chapter 4: Updated sections 4.1, 4.2, 4.3, 4.4. Updated table 4-1 and figure 4-1.
		Chapter 5: Updated sections 5.1, 5.2, 5.3. Added new figure 5-7 for Threat Vignettes
		Chapter 6: Updated sections 6, 6.3, 6.4. Updated tables 6-1 and 6-2
		Chapter 7: Updated section 7, 7.1, 7.3
		Chapter 8: Updated section 8, 8.1, 8.2, 8.3; updated figure 8-1
		Chapter 9: Updated for use of Red Teams, section 9, 9.3, text box in 9.3.1; updated figure 9-1
		Chapter 10: Added acronyms; corrected CSA, CSRC; updated glossary
		Chapter 11: Updated and added references
		Appendix A: Updated terminology
		Appendix C: updated table C-1
		Appendix G: Updated figure G-6

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, system cyber survivability, and operational 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. The guidebook includes footnoted references for some content to assist with understanding the source of the content.

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 Program Managers (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/resp/CTT>

1.2 Audience

This guidebook is intended for PMs, Chief Developmental Testers (CDTs), Lead Developmental Test and Evaluation (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, industrial control systems [ICS], hull, mechanical and electrical [HM&E] systems, and supervisory control and data acquisition [SCADA] systems) regardless of their acquisition category (i.e., [Acquisition Category] ACAT I, IA, II III, IV and BCAT I, II, III) or their phase of the acquisition life cycle unless noted. Acquisition cybersecurity T&E is not a stand-alone domain but is part of the overall program T&E strategy.

Acquisition programs not required to follow DoD Instruction 5000 series guidance will also benefit from following this guidebook.

1.4 Terminology

Cybersecurity T&E 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 operational resilience and system cyber survivability capabilities within a mission context.

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, government and contractor/developers, involved in the verification and validation of system cybersecurity capabilities, system cyber survivability, and operational resilience requirements across the life cycle of a system. Appendix F 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 survivability and operational resilience. This guidebook uses the phrase Prevent, Mitigate, Recover (PMR) for consistency with the key attributes described in the Cyber Survivability Endorsement Implementation Guide (CSE IG)¹. 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 CSE IG is found in this guidebook in Section 2.4 and Appendix X1.

¹ *Cyber Survivability Endorsement Implementation Guide (CSE IG) version 2.01, Joint Staff*

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

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 should 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.”² 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 Fiscal Year 2016 National Defense Authorization Act (NDAA) Section 804

In 2016, Congress passed the Section 804 National Defense Authorization Act, titled *Middle Tier of Acquisition for Rapid Prototyping and Rapid Fielding*³ that addresses using innovative technology to rapidly develop fieldable prototypes and field capabilities within 5 years of an approved requirement to demonstrate new capabilities to meet emerging military needs. Middle Tier Acquisition (MTA) programs are exempt from DoDI 5000.02 and Joint Capabilities Integration and Development System (JCIDS) processes but are not exempt from requirements approval.

MTA programs may field a prototype that can be demonstrated in an operational environment and provide residual operational capability within 5 years of an approved requirement. MTA programs may also use a rapid fielding pathway for rapidly fielding production quantities of new or upgraded systems with minimal development required. The objective of a rapid fielding program is to begin production within 6 months and complete fielding within five years of the requirement.⁴ A rapid acquisition program can proceed from approved requirement directly to production with minimal development or as a follow-on to a rapid prototype.

Section 804 MTA programs require tailored cybersecurity T&E processes that keep pace with rapid acquisition and fielding timelines. This implies early planning and analysis to ensure the analysis of alternatives (AOA) research includes cybersecurity requirements for evaluating alternatives and the prototype Requests for Proposals (RFPs) include contractor cybersecurity T&E requirements. Cybersecurity T&E planning will require automated cybersecurity testing for software, but also should include test tools and test engineers embedded in the system development process. Appendix C describes test tailoring for MTA programs.

² DoDI 5000.02, *Operation of the Defense Acquisition System*, Enclosure 14 (7 January 2017)

³ National Defense Authorization Act for Fiscal Year 2010, 10 U.S.C., Pub. L. 111-84 § 804 (2009)

⁴ USD(R&E) *Middle Tier of Acquisition (Rapid Prototyping/Rapid Fielding) Interim Governance*, (October 9, 2018)

2.3 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 is that the BCAC has different phase names and six milestone decisions (depicted in Figure 2-1) instead of three.

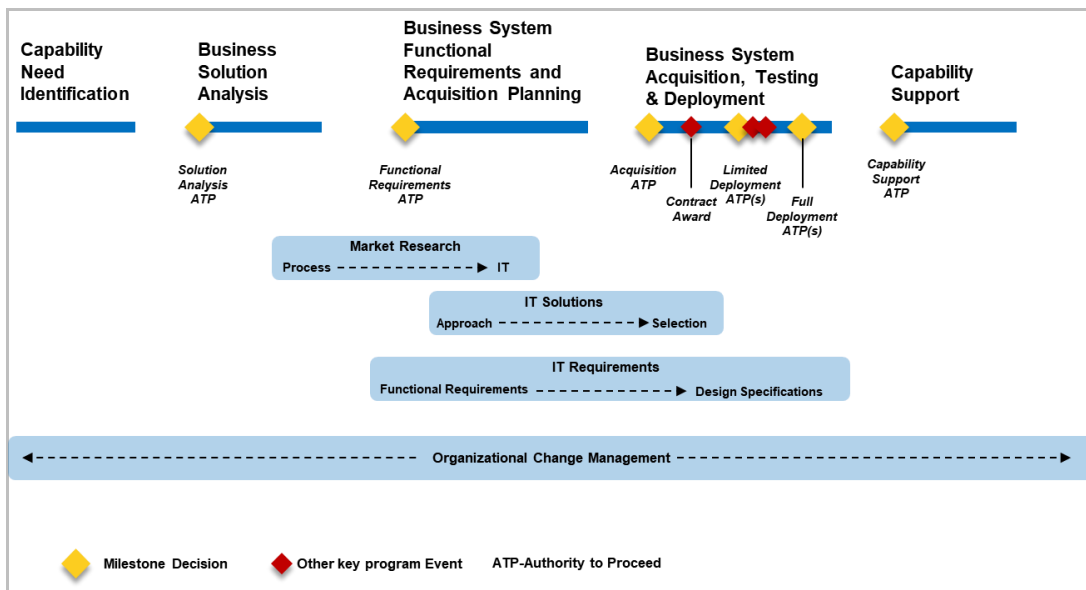


Figure 2-1. Business Capability Acquisition Cycle

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 Developmental Test and Evaluation Framework (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) Memorandum—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.

2.4 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, risk management, 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 (SP) 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 them 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 should test procedures and tactics for workarounds and fallbacks in hostile environments. PMs should:

- Conduct periodic exercises or evaluations of a program's ability to operate during loss of all information resources and connectivity.
- Ensure that systems can allocate information resources dynamically as needed to sustain mission operations while addressing cybersecurity failures, no matter the cause.
- Ensure that 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 should 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 should 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 that PMs successfully perform the above defined DoDI 8500.01 activities.

2.4.1 Risk Management Framework, DoDI 8510.01

The RMF, defined in NIST SP 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 related to RMF and DT&E but does not replace specific DT&E or OT&E guidance. 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

2.5 Cybersecurity Activities Support to DoD Information Network Operations (DODIN), DoDI 8530.01

DoDI 8530.01 “*The Cybersecurity Activities Support to DODIN*” supports RMF requirements to monitor security controls continuously, determines the security impact of changes to the DODIN and operational environment, and conducts remediation actions as described in DoDI 8510.01. DoDI 8530.01 applies to DoD IT (e.g., DoD-owned or DoD-controlled information systems (ISs), platform information technology (PIT) systems, IT products and services) as defined in DoDI 8500.01 and control systems and industrial control systems (ICSs) as defined in NISTSP 800-82 that are owned or operated by or on behalf of DoD Components. DoDI 8530.01 also applies to cleared defense contractors and any mission partner systems connecting to the DODIN.



Cybersecurity T&E should verify and validate that the appropriate security measures were effectively integrated into the system boundary by testing Defensive Cyber Operations (DCO) defensive measures during test events. Testing DCO defensive measures allow mission owners and operators, from the tactical to the DoD level, to have confidence in the confidentiality, integrity, and availability of the DODIN and DoD information to make decisions.

2.6 Joint Requirements Guidance

In January 2017, the Joint Requirements Oversight Council (JROC) approved a proposed update to the JCIDS manual (ref. JROCM 009-17) that updates the System Survivability Key Performance Parameter (SS KPP). The SS KPP update encourages requirements developers to leverage the CSE IG 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 CSE IG consists of guidance that helps acquisition programs ensure that 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 (SSEs) to define the 10 cyber survivability attributes and risk-managed performance measures in their functional and system requirements documents.

Several Services have similar standards for cybersecurity T&E. The Navy has established the CYBERSAFE process to ensure overall resilience in addition to the RMF process. The Air Force promulgated an update Air Force Instruction (AFI) 99-103 where cybersecurity testing is prominent in the policy for aircraft testing.



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

2.7 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 development contractor, developmental testers, and operational testers in test analysis and planning. Each cybersecurity T&E phase is iterative and includes Phase 1 and 2 ongoing planning and analysis activities for the subsequent phases. For example, before Phase 5, the contractor and government test teams should repeat Phases 1 and 2 to ensure the requirements are clear and concise and understand any updates to the attack surface. Changes in the attack surface will help identify the CVPA scope to a greater fidelity. Tools that can automate the Phase 1 and 2 activities and that include a digital model of the systems and integration points may facilitate a faster planning and analysis effort. When referred to in this Guidebook, the system developer or system integrator may be a government or contractor or shared role.

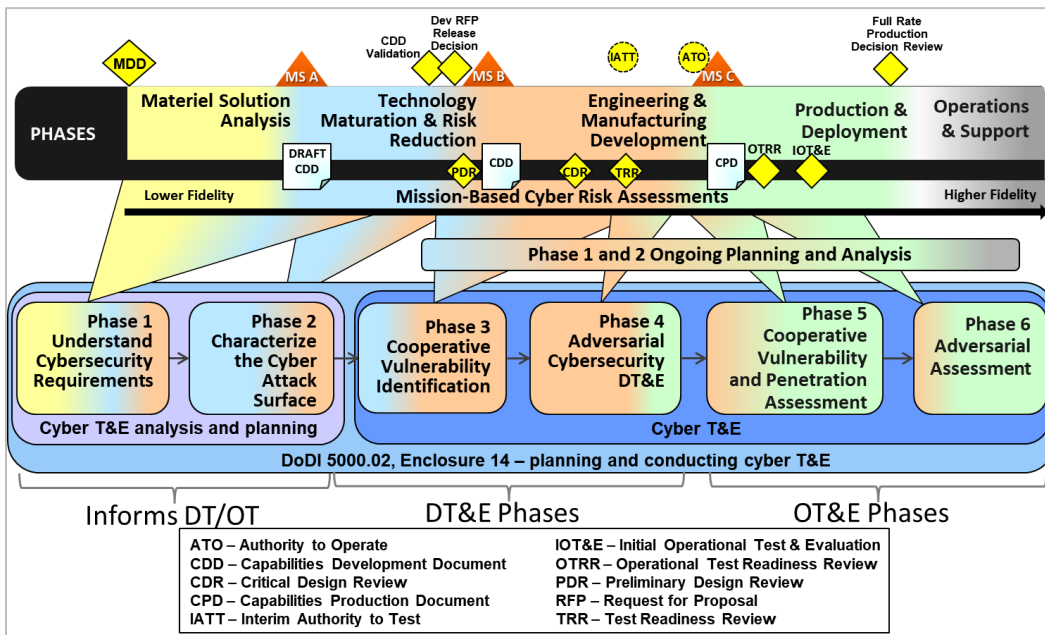


Figure 3-1. Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle

- Phase 1—Understand the Cybersecurity Requirements. The purpose of the Phase 1 is to examine the system’s cybersecurity, system cyber survivability, and operational resilience requirements for developing initial and subsequent approaches and plans for conducting contractor and government cybersecurity T&E.
- Phase 2—Characterize the Attack Surface. During Phase 2, government and contractor test teams identify vulnerabilities and avenues of attack an adversary may use to exploit the system and develop plans to evaluate the impacts to the mission.
- Phase 3—Cooperative Vulnerability Identification. The purpose of the third phase is to begin testing early to verify cybersecurity and operational resilience and identify vulnerabilities and inform implementing any needed mitigations. Using multiple tailored test events, vulnerability identification informs contractor and government system designers, developers, and engineers of

needed system cyber survivability and operational resilience improvements to reduce risk. Phase 3 is iterative during contractor development and includes regression testing to verify implemented mitigations. Phase 3 is also iterative during government DT&E.

- Phase 4—Adversarial Cybersecurity DT&E. During this phase, integrated contractor and government adversarial test teams test critical functionality. Cybersecurity and operational resilience testing are conducted during system development using a mission context. Phase 4 is iterative during contractor system development.
- Phase 5—Cooperative Vulnerability and Penetration Assessment. The purpose of this phase is to use data from cooperative cybersecurity test events to characterize the cybersecurity and resilience of a system in an operational context and provide reconnaissance of the system in support of the AA. This Phase includes assessing all test data from prior testing and is not a single test event.
- Phase 6—Adversarial Assessment. Phase 6 characterizes the operational mission effects to critical missions caused by threat-representative cyber activity against a unit trained and equipped with a system, as well as the effectiveness of defensive capabilities.

The goal of cybersecurity T&E is to identify and mitigate exploitable system vulnerabilities impacting operational resilience of military capabilities before system deployment to include safety, survivability, and security. Early discovery of system vulnerabilities can facilitate remediation and reduce impact on cost, schedule, and performance. Cybersecurity T&E Phases 1 and 2 are the essential first steps of the T&E planning process that support system design and development. Phase 1 and 2 should be performed in a cyclic fashion and repeated throughout each phase to ensure a thorough understanding of the requirements and any changes within the attack surface. 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) and specialized component engineers during the early stages of prototyping, system design and development to facilitate design changes that improve cybersecurity, system cyber survivability and operational 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. Integrating developers and engineers for specialized components or functionality with the testers is also important to design effective, relevant testing.

Detailed test planning and execution occurs during system prototyping, system development and prior to system deployment. The various planned test events are aligned to Phases 3, 4, 5, and 6, depending on the acquisition life cycle and purpose of the testing. Phases 3 and 4 comprise cybersecurity DT&E execution activities for all sub-components and component integration during prototype development, system development, up through the full system delivered to the government for independent DT&E. Contractor and government 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. Operational cybersecurity testing supports the evaluation of system effectiveness, suitability, and survivability. The OTA follows the procedures promulgated by DOT&E to plan for and conduct Phase 5 and 6 activities. OTAs will require results from DT&E Phases 1 and 2 analyses and all DT&E test results to inform the OTA Phases 1 and 2 updates and cybersecurity OT&E.

During Operations and Support (O&S), PMs should periodically reevaluate systems for cybersecurity, system cyber survivability and operational resilience. The CSE IG requires all programs implementing the CSE to include Cyber Survivability Attribute (CSA) 10: Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP). CSA 10 will necessitate an iterative effort to repeat Phases 1 and 2, plan additional testing if needed, and potentially

re-engineering to address needed mitigations. Previously discovered and un-mitigated low risk to mission vulnerabilities over time may become high risk and system updates and changes in interfacing systems may introduce new exposures and risk. Phases 1 and 2 help to plan and scope government-conducted sustainment testing. Sustainment testing should take continuous monitoring data into account and may inform changes in people, processes or technology in order to mitigate risk.

Follow on Operational Test and Evaluation (FOT&E) is part of the O&S process and may include re-assessing test activities and test data from previous assessments. FOT&E is a vital part of assessing operational resilience. The continual PMR capabilities should be evaluated during FOT&E. There may be other reasons to return to formal T&E other than program-initiated system modifications:

- Help ensure adequate funding is planned for the O&S phase through the future of the program
- Changes and modifications to the system as part of a system of systems, especially interfaces that may not be under control of the system, for example if a mission planning system is modified, the processes and systems supported by the mission plan may be impacted
- Changes to threat capabilities, newly revealed vulnerabilities, and new threat vectors

At a minimum, the program 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 system's ATO. The Life Cycle Sustainment Plan (LCSP) should include cybersecurity T&E.



3.1.1 Iterative Nature of the Phases

Cybersecurity T&E phases are iterative (i.e., activities should be repeated multiple times due to changes in the system architecture, new or emerging threats, and changes in the operational environment). Here are some common examples of events that would drive iteration of the phases:

- 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 Phases 1 and 2 to incorporate any changes that may impact test planning and before conducting the next set of testing in any of the phases.
- Updates to the TEMP or other test strategy documents concurrently with SE activities to update requirements, architecture, and design would necessitate Phases 1 and 2 iteration.
- Changes to the target operational environment that may drive changes in design and subsequent test strategy which may impact the cyber-attack surface (Phase 2), and test planning for Phases 3, 4, and 5.
- Changes to the cyber threat environment, if significant, may trigger repeat of Phase 2 attack surface analysis
- When testers verify cybersecurity and operational resilience and discover new high-risk vulnerabilities, the PM may need to update requirements to mitigate the discovered vulnerabilities. Phases 1 and 2 should be repeated to examine the updated cybersecurity requirements and assess any changes to the system's attack surface.

Figure 3-2 depicts phase iteration after initial testing during Phase 3 and after Phase 4. Phases 3 and 4 are iterated in a find-fix-verify method (described later in chapters 6 and 7).

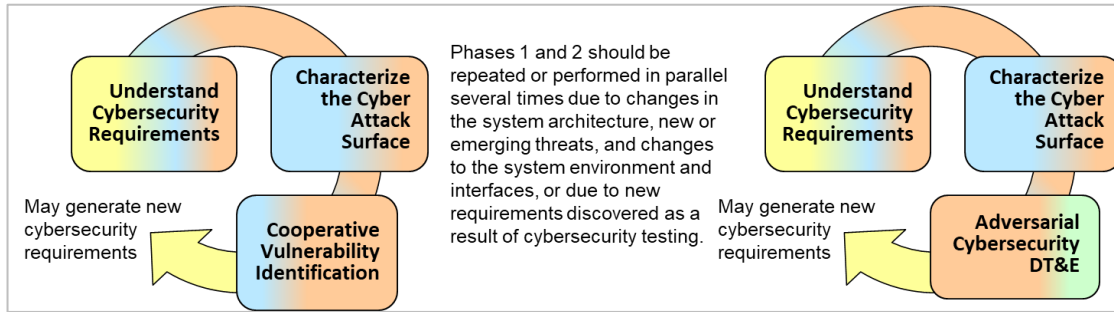


Figure 3-2. Cybersecurity T&E Phases Are Iterative

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. 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, and resources to include funding for integration of contractor and government cybersecurity testers, to the early analysis that the phases identify (understanding the cybersecurity requirements and characterizing the attack surface) to establish the foundation for efficient cybersecurity standards, system cyber survivability and operational resilience testing. Appendix C describes tailoring considerations for cybersecurity T&E phases and provides examples for DBS that use the BCAC, smaller acquisition programs, Section 804 MTA programs, and other 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 that 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 guides 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 CyWG membership should reflect the system type and size of program to include program specific cybersecurity staff.



The recommended participants in the CyWG are:

- CDT or system test lead if the CDT has not yet been appointed
- SSE
- ISSM
- Lead Systems Engineer Representative
- Lead Software Engineer/Architect
- Lead DT&E Organization Representative

- Critical or specialized sub-component, component or functionality developers and engineers
- Operational Test Agency Representative
- Cybersecurity DT&E Technical Experts (testers/analysts/assessors)
- Cybersecurity OTA Technical Experts (testers/analysts/assessors)
- Security Controls Assessor (SCA)
- Cybersecurity Subject Matter Experts (SMEs)
- Cyber-Intelligence SME
- Software Assurance Testing SME
- Scientific Test and Analysis Techniques (STAT) and/or Design of Experiments SME
- Cyber Test Range Representative
- Modeling and Simulation SME
- Anti-tamper (AT) Representative
- Interoperability Engineers, Representatives and Testers
- CSSP and DCO Representatives
- Active Duty System Operators
- System Maintainers and Logisticians
- Service-Specific T&E Policy Representative, if needed
- Oversight organizations and stakeholders, if appropriate
- Developers
- 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. It is critical to involve Cyber-Intelligence SMEs in this discussion to identify accurate threat intelligence for the specific system to be tested. The CyWG recommends an appropriate frequency for conducting cybersecurity threat assessments throughout the system development life cycle, but at a minimum, the Program Office obtains a validated threat assessment (e.g., Validated Online Lifecycle Threat [VOLT] report or Service/Component threat assessment report) from the DIA 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, SSEs, and SE helps acquisition programs avoid costly, difficult system modifications late in the acquisition life cycle. The CDT or system test lead should collaborate with SSE and SE providing architecture and design information and derived critical technical parameters (CTPs) including requirements traceability throughout the system life cycle to the CDT. Requirements traceability documentation provides insight into the design decisions for allocating

cybersecurity requirements which gives testers context to develop more tailored tests. The CDT will use this information to inform T&E activities and scenarios, to include what testing and 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.

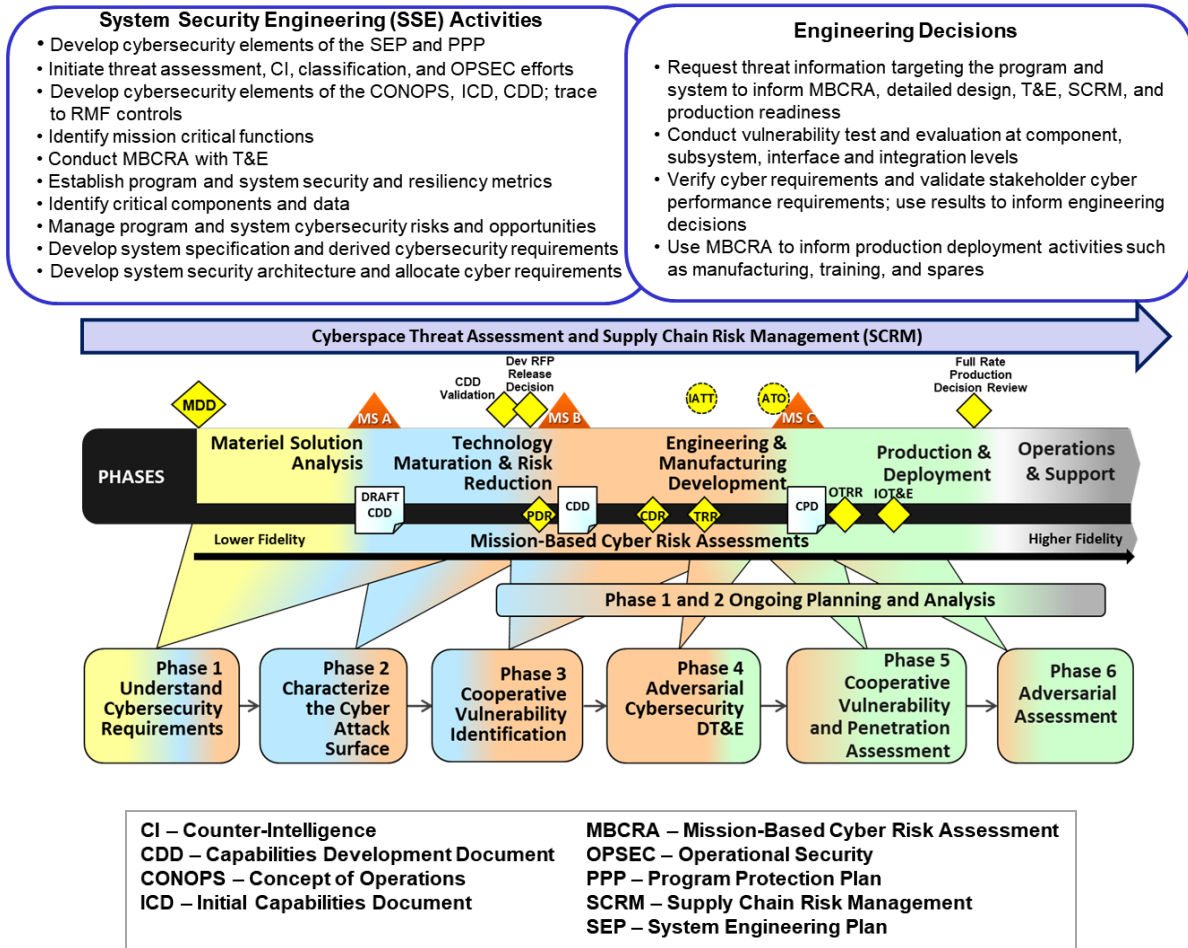


Figure 3-3. Interaction of SE and T&E Cybersecurity Activities

SSE and SE derive CTPs required for test planning. Figure 3-3 illustrates the interaction between cybersecurity T&E activities and SSE 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 integrate SSE, SE and T&E into the program’s acquisition strategy using the applicable DoD policy and guidance.

T&E, SSE, and SE should collaborate early to conduct MBCRAs/Cyber Table Top (CTT) exercises, described in Appendix X3, to inform the design of a system and increase the operational resilience of that system in its intended cyber-contested environment. Early T&E and SE collaboration is important because the contractor will build and test to the requirements only, ensuring that the system meets specifications. There may be implied or derived requirements that necessitate further discussion to accurately relay them to the contractor. During Phase 1 and 2, cybersecurity testers examine cybersecurity mission risk and cybersecurity, system cyber survivability, and operational resilience requirements based on the content of the system’s SE design documents to target systems for test activities.

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 should review and provide input to the PPP and plan testing to verify the effectiveness of the countermeasures. Contractors need to be informed of what the CPI of the system is and engineer a design that protects CPI from external and internal threats (this includes where/how they maintain system design environments). SSEs and SEs need to inform the contractors of the mission critical functions and ensure that they are prioritized correctly to achieve an adversary tolerant, operationally resilient system design.

The CyWG is the body of experts that enables SE, SSE and T&E to collaborate on cybersecurity, system cyber survivability and operational resilience issues. During the test planning process, the ISSM works with the CDT, SE, and SSE to identify and schedule all cybersecurity test and RMF activities. Integrating the adversarial and vulnerability test teams with the system engineers and developers (via the CyWG) allows the PM to design system cyber survivability and operational resilience into the functional mission system. To inform system designs, system engineers focus on mission capabilities, functional resilience, safety, and cybersecurity threats. Cybersecurity testers supplement SE and SSE knowledge by assessing threats and vulnerabilities inherent to the system designs. Adversarial cybersecurity testing informs SE and SSE of the system cyber survivability, cybersecurity and operational 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 contractor (when selected for prototypes or actual system development) and government cybersecurity testers/analysts, including OTAs, vulnerability assessment teams, and Red Teams, shortly after acquisition program initiation and before MS B. Program Managers should plan for funding this support by addressing this need in the acquisition strategy. Cybersecurity T&E planned early contributes to more cost-effective development of operationally resilient, survivable systems. During Phase 1, cybersecurity testers analyze architectures, system designs, and key interfaces to expose any additional implied and essential cybersecurity, system cyber survivability and operational resilience requirements. Testers also identify the T&E data needed to assess progress toward achieving cybersecurity, system cyber survivability and operational resilience requirements.

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

- Helps shape emerging system cyber survivability and operational resilience requirements, ensuring testable, measurable, and achievable requirements defined through the SE process and 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 AoA, RFPs and Statements of Work (SOWs), including specific cybersecurity and operational resilience testing tasks and Contract Data Requirements Lists (CDRLs). Appendix B provides additional information for cybersecurity T&E contract recommendations.
- Ensures that system cyber survivability and operational resilience requirements are consistent with the mission and threat conditions.
- Advises PMs and conducts early testing and analysis to identify any systematic cybersecurity, system cyber survivability, and operational resilience issues; conducts mission-based cybersecurity risk analysis, provides timely mitigation recommendations for fixes and verifies fixes which reduces risk of system re-design and modification.

- Identifies cybersecurity, system cyber survivability and operational resilience deficiencies 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, system cyber survivability, and operational resilience requirements for development and testing.
- Ensures test processes and data collection requirements, instrumentation, scheduling and planning for specialized environments/use of contractor or government labs are planned well in advance.
- Ensures early planning for cybersecurity, system cyber survivability, and operational 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 MBCRA(s) 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 informs PMs about the relevance of technical vulnerabilities affecting functional mission execution and operational resilience. Cybersecurity DT&E activities are not one-time activities that provide static information. Organizations should include in their prototype and development contracts the requirement for ongoing DT&E activities throughout the system development life cycle before government product acceptance testing. The frequency of DT&E activities depends on the defined purpose and scope of assessments required during system development. PMs should develop a cybersecurity T&E strategy based on system cybersecurity requirements, derived system requirements, and draft system performance specifications. The strategy should include contractor cybersecurity DT&E of sub-components, components, integrated components and full system vulnerability and threat-based testing prior to program product acceptance testing.

Cybersecurity DT&E evaluates a system's mission performance in the presence of cybersecurity threats and informs acquisition decision makers regarding the system's ability to meet cybersecurity standards, the system's level of operational resilience to support mission operations, and system cyber survivability. CDTs and T&E Leads should plan contractor cybersecurity DT&E in all three areas.

These three sets of testing requirements overlap and include contractor and government testing of people, processes and technology. The three sets of testing requirements are depicted conceptually in a Venn diagram in Figure 3-4. The circles of the Venn diagram change size depending on the mission focus of the system under test. For example, DoD weapon systems may place special emphasis on the system's operational resilience (the system's ability to support mission operations consistent with mission performance parameters). If the system under test (SUT) has a SS KPP requirement, system cyber survivability may be the highest consideration for cybersecurity testing, with operational resilience and cybersecurity standards a secondary focus. When all three sets of requirements are of equal importance the circles are equal as shown in Figure 3-4. The degree of overlap will vary depending upon the type of

system. For example, a defense business system may have nearly concentric circles for system cyber survivability and cybersecurity standards and high overlap with operational resilience. On the other hand, a weapon system may have far less overlap. At the intersections of each pair of requirements, testing should specifically focus on defensive cyber operations capabilities and interoperability, as required in DoDI 8500.01 and described in DoDI 8530.01 and DoDI 8330.01. Derived system requirements and system performance specifications support DoDI 8500.01 policy.

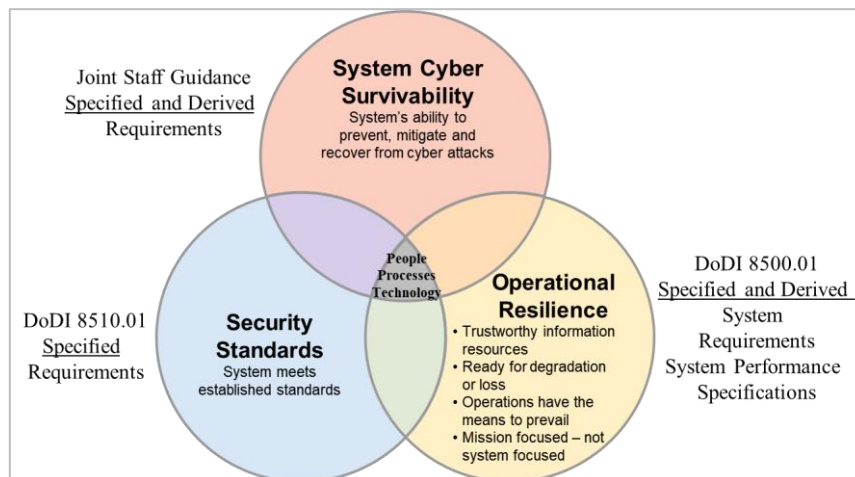


Figure 3-4. Cybersecurity Testing Requirement Venn Diagram

3.7.1 Testing Security Standards

Security standards can be found in numerous DoD policies. Not all systems have the same cybersecurity requirements. Following the “Identify” function of the NIST Cybersecurity Framework, the first step in planning cybersecurity testing (analogous to Phase 1) is to identify the policies, procedures, and processes to manage and monitor the system’s cybersecurity requirements. Existing policies can be found on the cyber policy chart located at: <https://www.csiac.org/resources/the-dod-cybersecurity-policy-chart/>.

Since not all standards apply to all systems, this Guidebook will discuss only the standards that are required by all DoD IT (e.g. DoD-owned or DoD-controlled information systems, platform information technology (IT) systems, IT products and services). Chapter 11 lists the relevant DoD-wide cybersecurity standards and cybersecurity T&E standards. RMF and DCO are two such sets of standards with established policy, guidance and cyber requirements that are required for all DoD IT.



3.7.1.1 Testing RMF Standards

Cybersecurity standards as used in this guidebook are the security controls required by the RMF process and adhere to DoDI 8510 as specified requirements. Cybersecurity DT&E includes RMF assessment activities and a thorough evaluation of the system’s cyber survivability and operational resilience posture with respect to the security controls implementation.



RMF A&A is necessary but not sufficient to ensure that a system can operate in a cyber-contested environment. The RMF assessment process evaluates if individual planned security capabilities are in place and in compliance with standards, but it does not test how well the security capabilities in an integrated aspect work in the presence of a cyber-threat during mission execution. Nor does it assess if the holistic set of standards compliance result in unforeseen risks resulting from the complex interdependencies within the system, or across system of systems, including risk from outside of the system ATO boundary. By integrating RMF assessment activities with cybersecurity DT&E starting with prototyping and development contracts, the Program Office completes a thorough evaluation of the system’s cybersecurity and resilience posture and better informs decision makers and Authorizing

Officials (AOs) about the risks to mission execution. During the test planning process, the ISSM works with the CDT, SE, and SSE to identify and schedule all cybersecurity test activities.

During system development, contractors verify the function of security controls and government cybersecurity DT&E product acceptance testing validates the implementation of security controls and performance parameters. Contractor and government testing occur before formal security controls assessment to ensure that controls operate as intended when they are initially developed. This allows time to remediate any defects discovered and re-verify the security control functions as intended. Phases 2, 3, and 4 of the cybersecurity T&E process provide data to contractor SSE and SE as well as government SSE, SE and the ISSM. This data informs and supports execution of RMF processes and informs additional, modified, or strengthened countermeasures and controls. Cybersecurity T&E test data also informs RMF continuous monitoring processes and DCO processes.



After DT&E, test reports may inform the SCA, SE or SSE, and AO on the sufficiency and/or compliance of controls after analysis is conducted on the test results. Figure 3-5 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.

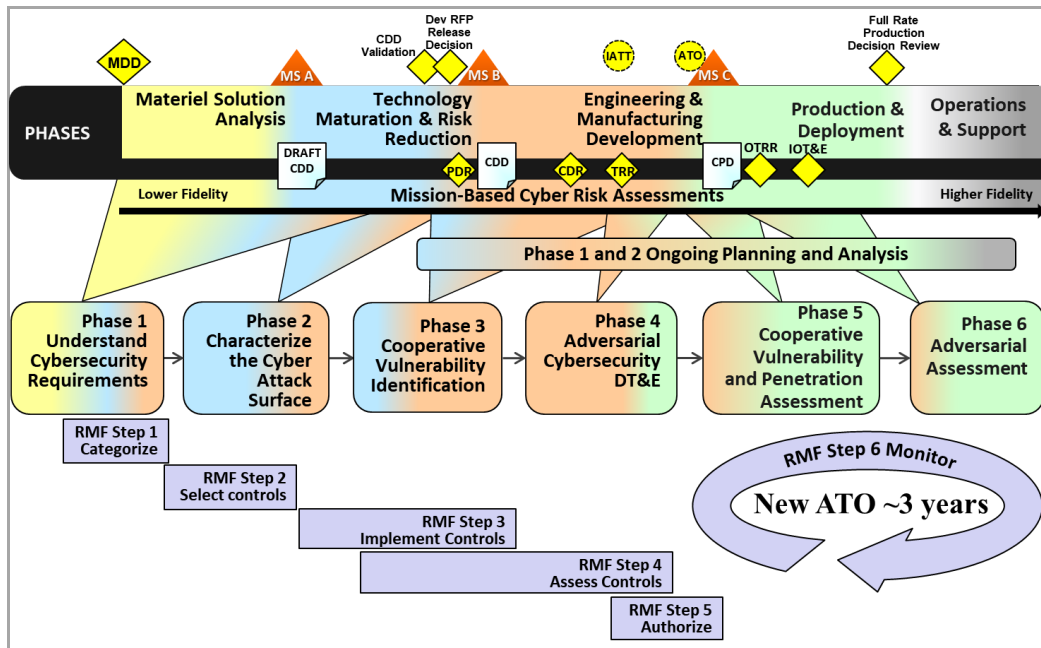


Figure 3-5. Interaction of RMF and T&E Cybersecurity Activities

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 and validation 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 or cyber range events do 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 should be assessed for the IATT.
- The security controls that the contractor should design, develop, and assess for inclusion in the Development RFP.
- The order in which security controls should 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.

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.

3.7.1.2 Testing Defensive Cyberspace Operations Standards

DoD integrates the following cybersecurity activities to support DoDIN operations and DCO internal defensive measures in response to cyber vulnerabilities and threats:

- Vulnerability assessment and analysis
- Vulnerability management including patch management
- Malware protection
- Continuous monitoring
- Cyber incident handling
- DoDIN user activity monitoring for the DoD Insider Threat Program
- Warning intelligence and attack sensing and warning

DCO standards are focused on the maturity levels of cybersecurity activities required by DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* and detailed in the *Evaluator Scoring Metrics*. All DoD IT is required to ensure alignment to a Network Operations Security Center or authorized CSSP for cybersecurity services as a condition to grant an ATO. The program office should coordinate with the DCO provider to determine which responsibilities and requirements will be organically provided, and which will be outsourced to the provider through signed agreements. The CSSP's responsibilities and the subscriber's responsibilities for each cybersecurity service will be specifically assigned and documented in the contract.

Each DCO activity requires people, processes, and technologies that are designed into the system and assessed for performance and effectiveness. During design and development, a defense-in-depth strategy should be developed to identify and assess the required technologies needed at the system perimeter, within the network, at the endpoint and at the data level to prevent, mitigate, and recover from cyber-attacks. The development contract should clearly state the contractor's role in designing to and developing this strategy.

During contractor and government cybersecurity testing, each capability identified in the defense-in-depth strategy should be evaluated on measures of performance and the measures of effectiveness within the scope of the system's mission. For example, simply having an intrusion detection system is of no benefit if the penetration attempts are not logged by the system, or not recognized by operators. DT&E should include DCO testing whenever possible to:

- Maximize tuning of the tools for effective detection
- Establish a baseline of normal versus anomalous activity

- Provide operators/technicians experience recognizing cyber-attacks

3.7.2 Testing Operational Resilience During Cyber-Attacks

Operational resilience is an implied requirement for all DoD systems and is defined in DoDI 8500.01. The requirement to be operationally resilient implies that the system is designed to protect mission essential components, detect cyber-attacks, and, whenever possible, be able to reconfigure, optimize, self-defend, and recover with little or no human intervention and produce an audit trail of these incidents. Program protection planning is intimately linked with operational resilience by describing how the components will be protected.

The requirement for operational resilience addresses the system's ability to:

- Operate during loss of all information resources and connectivity
- Allocate information resources dynamically as needed to sustain mission operations while addressing cybersecurity failures
- Restore information resources rapidly to a trusted state while maintaining support to ongoing missions

For systems to be operationally resilient, resilient capabilities are articulated in the system specifications, and may need to be tested and assessed starting at the individual component level to full up system testing. Cybersecurity DT&E ensures the specifications have been satisfied. These specifications may differ from cyber system survivability and security standards specifications in that operational resilience specification language should specify mission and functional performance relevant to operational missions as opposed to information technology performance.

Testing for operational resilience may also include examination of the safety aspects of the system that could be impacted by a cyber threat. The components of operational resilience also span staff roles and responsibilities, Concept of Operations (CONOPS) processes for mission recovery, and technology components such as redundant systems and networks, and system capabilities for failover. Testers should first understand the requirements and design components associated with operational resilience and ensure they are testable, measurable, and achievable. CDTs should evaluate operational resilience through the analysis of a system's operational resilience Technical Performance Measures (TPMs). OT&E then determines if the system is operationally effective, suitable and survivable. For more information about TPMs, refer to Appendix X1. This Guidebook describes information in each cybersecurity testing phase for conducting this testing.

3.7.3 Testing System Cyber Survivability During Cyber-Attacks

The CSE IG consists of guidance that helps acquisition programs ensure that cyber survivability requirements are included in CDDs and early system designs and that cyber survivability requirements are measurable, testable and achievable. The pillars of cyber system survivability are:

- *Prevent* – design principles that protect system's mission functions from most likely cyber threats
- *Mitigate* – design principles to detect and respond to cyber-attacks; enable the mission system to survive attacks and complete the mission
- *Recover* – design principles to enable recovery from cyber-attacks and prepare mission systems for the next fight

The Recover pillar may significantly overlap with the operational resilience requirements. The CSE IG identifies 10 high-level CSA that can be tailored to support system-specific, measurable and testable

cyber survivability requirements for PMR. The scope and implementation strength of the CSAs are determined by the Cyber Survivability Risk Category (CSRC). The CSRC is a function of⁵:

- Selecting the system’s mission type
- Determining the relevant threat actor(s)
- Determining the system’s cyber dependence
- Determining the impact of system compromise to the supported mission(s)

Underpinning the CSAs are security controls that should be designed into the system and then tested to ensure that the needed level of cyber survivability to support the SS-KPP is achieved. Note that measurement of how well a system meets CSAs is not a measure of system cyber survivability. OT&E determines if the system is operationally effective, suitable and survivable.

For more information about the CSAs and the process for determining a CSRC and using it to determine system requirements, refer to the CSE IG⁶. A summary of the 10 CSAs is shown in Table 3-1:

Table 3-1. SS KPP Pillars and Cyber Survivability Attributes (CSAs)

SS KPP Pillars (Mandatory)	Cyber Survivability Attributes (CSA) (All considered, then select applicable subset)
Prevent	CSA-01 - Control Access
	CSA-02 - Reduce System’s Cyber Detectability
	CSA-03 - Secure Transmissions and Communications
	CSA-04 - Protect System’s Information from Exploitation
	CSA-05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels
	CSA-06 - Minimize and Harden Attack Surfaces
Mitigate	CSA-07 - Baseline & Monitor Systems and Detect Anomalies
	CSA-08 - Manage System Performance if Degraded by Cyber Events
Recover	CSA-09 - Recover System Capabilities
All (Prevent, Mitigate, and Recover)	CSA-10 - Actively Manage System’s Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP)

To test a system’s cyber survivability during DT&E, CDTs and test leads should design test objectives to assess the system’s ability to prevent, mitigate and recover from cyber-attacks within a mission context using the CSAs. The CSRP in CSA 10 is a mission relevant assessment across all the CSAs to evaluate the overall risk posture. CyWGs should plan for collecting the data, specifying the assessment criteria and tracking the CSRP throughout the life cycle. This Guidebook describes information in each cybersecurity testing phase for conducting this testing.

3.8 Integrated Testing

Integrated cybersecurity 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 T&E planning enhances the operational realism in DT&E, providing opportunities for early identification of system design improvements. Integrated test activities include contractor assessments and test activities.

⁵ *Cyber Survivability Endorsement Implementation Guide v2.01*, Joint Staff Publication

⁶ Ibid

Integrated T&E does not replace or eliminate the need for dedicated DT&E or dedicated Initial Operational Test and Evaluation (IOT&E), as required by 10 U.S. Code (USC) 2399, *Operational Test and Evaluation of Defense Acquisition Programs*, for MDAPs. For more information about integrated T&E, see the Defense Acquisition Guidebook (DAG), Chapter 8.

To conduct integrated cybersecurity T&E, the CDT, CyWG, and OTA develop an integrated cybersecurity T&E strategy that includes cybersecurity DT&E, OT&E, and RMF assessment requirements. They also form an integrated cybersecurity test team consisting of DT, OT, and RMF representatives. This integrated test team should include the contractor cybersecurity test members as well as government test members and the testing should start during contractor test, to the greatest extent possible. The integrated cybersecurity test team examines testing requirements documented in the TEMP and creates common test objectives and test plans as early in system development as possible. This early planning enables the shared test objectives that will produce test data that can be shared by the integrated cybersecurity test team.



The CyWG helps to identify opportunities for integrated cybersecurity test events to satisfy DT&E and OT&E test objectives. 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. When leveraging a DT&E environment to satisfy OT&E requirements, the OTA should evaluate the emulated operational environment to ensure it is as operationally realistic as possible. Use of data for OT&E requires consideration of whether the system under test is production-representative and the conditions are operationally representative in the context of the question that the test is attempting to resolve.

OTAs are highly encouraged to participate in planning during the early phases of cybersecurity DT&E. When funded by the Program Office, OTAs may participate in the initial cybersecurity T&E Phases 1 and 2 as members of the CyWG to gain information about cybersecurity and operational resilience requirements, mission risks, key cyber terrain, and systems' potential attack surface. OTAs may repeat Phases 1 & 2 to help scope testing before executing OT&E events to ensure a thorough understanding of the cybersecurity requirements and understand any changes in the attack surface. The CDT or system test lead, developer, and OTA should work together 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.

Including the developer, 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's operational resilience.

Data Sharing and Data Reuse. Data sharing and reuse provides data from cybersecurity DT&E and RMF controls assessment to the SCA, AO and OT&E testers. Advance planning and authorization from DT&E, OT&E, and RMF representatives is needed to agree on test objectives and methods that will produce the required data. As part of the planning, the integrated cyber test team should identify data that may be available from all sources including contractor and government sources, RMF security controls assessments, security inspections, developmental tests in system integration labs, testing in operational environments, DCO assessments, and testing with systems and networks that representative end users operate. This collective data set supports evaluating the system's cybersecurity posture (results of the security standards testing), operational resilience posture, and system cyber survivability posture.



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 CTPs, 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 operational resilience evaluation after each test event. When a cybersecurity and operational resilience evaluation follow every test event, the PM is informed about the cybersecurity and operational resilience of the system at that point in time. Furthermore, cybersecurity evaluation supports verification and validation of cyber-related technical specifications and requirements. Assuming robust cybersecurity requirements, cybersecurity evaluations, the “E” of DT&E and OT&E, should cover the following topics:

- Was the system designed securely and key data protected?
- Were secure coding practices used during the software development process?
- Is the system/software/hardware developed using industry security best practices?
- Do cybersecurity implementation 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 cyber survivability or operational resilience?
- Can the system recover from cyber-attacks and intrusions?
- Do information and diagnostic tools provided to system operator’s function correctly to enable satisfactory identification, response, and recovery actions?
- How secure is the system design for operation in a contested cyber environment?
- How are mission-impacting vulnerabilities and deficiencies identified, addressed, and mitigated?
- Is the system resilient to malicious activity coming from connecting, enabling, or supporting systems and interconnections?
- How is the system protected when operating in the mission environment?

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.



4 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, system cyber survivability, and operational 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. The PM, CDT, OTAs, and the CyWG need to understand the requirements in order to scope testing, establish test objectives and plan for test infrastructure, required test articles, tools, instrumentation and data collection. Phase 1 analysis uses engagement and collaboration with system engineers and operators to facilitate design changes that improve operational 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 phases. Automated tools that ingest model-based systems engineering (MBSE) design can accommodate more efficient Phase 1 analyses.

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.

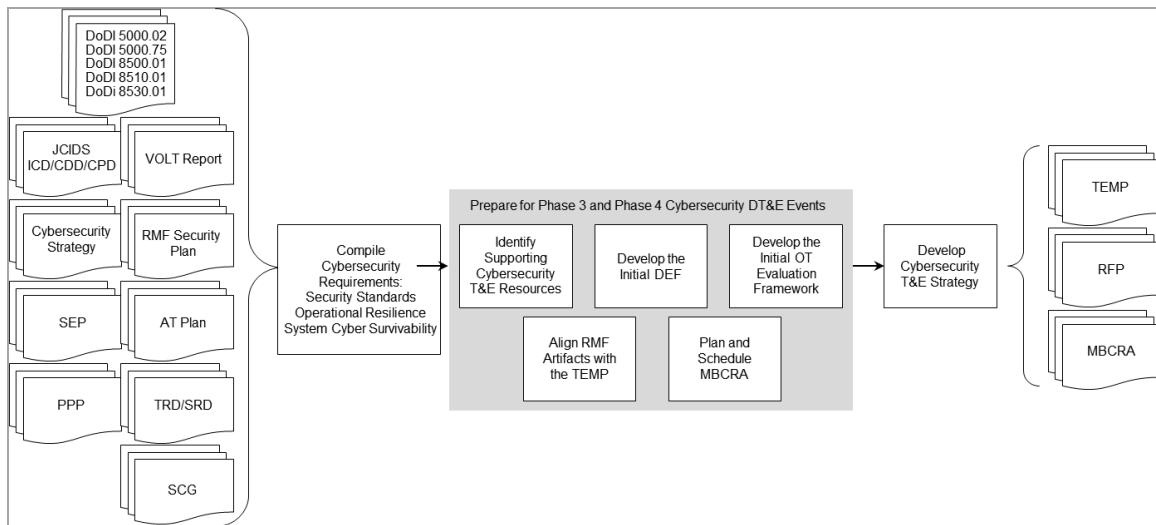


Figure 4-1. Phase 1: Understand Cybersecurity Requirements Activities

4.1 Schedule

Understanding cybersecurity, system cyber survivability, and operational 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 standards, system cyber survivability, and operational resilience requirements before it moves through each cybersecurity T&E phase. If no cybersecurity standards, system cyber survivability or operational 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 through the O&S 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.

In the case of late tester engagement, urgent operational needs, and rapid acquisition programs (rapid prototyping and fielding systems), Phases 1 and 2 may be performed in parallel. Phases 1 and 2 are essential for understanding what to test and how to test and therefore should not be skipped! PMs should ensure that program funding and acquisition strategies include the expectation that cybersecurity DT&E organizations and OTAs will require funding in order to support early and iterative Phases 1 and 2. Executing Phases 1 and 2 can provide useful information for understanding the operational trade space when developing a system, prototype, or capability. Accounting for cybersecurity requirements within this trade space is critical because if neglected it will negatively impact cost, schedule and performance.

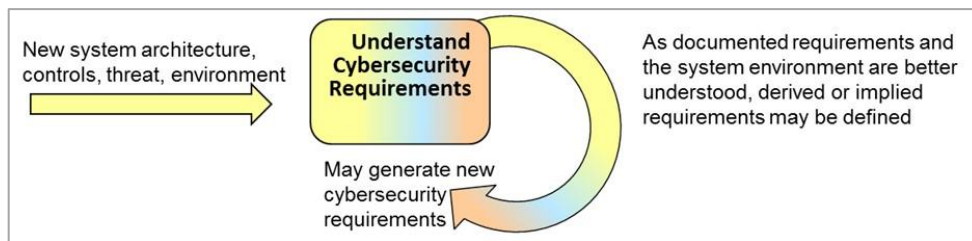


Figure 4-2. Phase 1 Iteration

4.2 Inputs

The following system artifacts are some of the inputs that can be used as available to gain an understanding of cybersecurity, system cyber survivability, and operational resilience requirements. These documents and artifacts are often updated throughout the acquisition.

- Capability Requirements Documents: JCIDS ICD, CDD, or CPD
- Mission CONOPS
- CSRC from CSE IG process
- DBS System Functional Requirements
- PPP including Criticality Analysis, Supply Chain and AT requirements, and Cybersecurity Strategy (DoD or Component CIO-approved document)
- SE Plan
- DoD Architecture Framework (DoDAF) System Views or MBSE artifacts
- DBS Design Specifications (if available)
- DBS Capability Implementation Plan (if available)
- VOLT report, Cyber Threat Modules (CTMs) from the Defense Intelligence Threat Library (DITL)
- Security Classification Guide
- RMF Security Plan, RMF Security Assessment Plan
- MBCRA, if available
- Previous cybersecurity vulnerability assessment reports, penetration testing reports or AA reports, if available
- CSSP Support Agreement
- LCSP



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. Depending on program size and phase in the acquisition cycle, not all these program documents are available and may be in other forms or have a different title. As Program Offices revise the documentation, Phase 1 should be iterated based on the updated documentation.

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 Standards, System Cyber Survivability, and Operational Resilience Requirements

As early and as often possible, the CyWG reviews system documentation to extract: 1) cybersecurity standards, system cyber survivability, and operational 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.

Examine Cybersecurity Standards. During Phase 1, the system receives an RMF categorization which determines the RMF controls the system should implement. The controls are engineered into the system design and are tested by the contractor. Government testers and SCAs verify the standards during later cybersecurity T&E phases. The developer environment, processes (i.e. software coding, updates) and tools must also be understood to identify areas where testing is needed. Later in development, the processes for maintaining the system will also need to be evaluated to understand risk, effects of updates on configuration management, DCO and CSSP responses, and to inform the life cycle sustainment and continuous monitoring plans. In addition to the system cybersecurity standards, the PPP should identify critical components and functionality to be protected in the supply chain. The CDT should understand areas of supply chain risk in order to plan related testing.



Examine Operational Resilience Requirements. During Phase 1, examine the operational requirements that support the system’s ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, cyber-attacks, or system compromises.

Examine System Cyber Survivability Requirements. If the system has an SS KPP, during Phase 1 the PM should ensure that the system also has a CSRC assigned and related CSAs. Examine applicable CSA requirements as described in the ICD or CDD. If the system does not fall under the JCIDS process, it is still highly recommended to tailor the CSAs in partnership with the Lead Systems Engineer. Refer to the CSE IG for further detail.

The documents listed as inputs in Section 4.2 provide information on the requirements and testing factors found in Table 4-1 below.

Table 4-1. Cybersecurity and Operational Resilience Requirements and Testing Factors to Consider

Requirements/Test Factors	Description	Why?	Where to Find
Mission operation in cyber-contested environments	Sets general expectations for operations in a cyber-contested environment.	Derive cybersecurity and operational resilience requirements from this statement to ensure required mission operation.	JCIDS Documents Technical Requirements

Cybersecurity Test and Evaluation Guidebook 2.0, Change 1

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



Requirements/Test Factors	Description	Why?	Where to Find
CSSP support agreement	The plan for DCO capabilities and services that will be organic and inherited.	Identifies requirements the program will have to meet for DCO. This includes people, processes and technologies required to enable a provider or an organic capability.	PPP/Cybersecurity Strategy appendix LCSP
Financial system requirements if applicable	DoD financial systems may contain cyber economic vulnerabilities and cyber economic SMEs should ensure that the key operational capabilities and business processes are evaluated.	Financial systems are required to conduct a CEVA in accordance with (IAW) DoDI 5000.02 and 5000.75.	JCIDS Documents TRDs
Cybersecurity risk categorizations	The Joint Staff's CSRC and the DoD CIO RMF Categorization.	The depth and breadth of cybersecurity T&E strategy should reflect the cybersecurity risk to the systems that these risk categorizations describe.	JCIDS Documents RMF Security Plan Cybersecurity Strategy
MBCRA results	If available, identifies the current cyber risk posture for the system.	Current risk posture of the system drives further T&E planning and focus to reduce risk.	MBCRA Document
Supply chain protection requirements	The PPP defines supply chain risks and how the program will manage risks to critical functions and components	Describes how supply chain threat assessments are used to influence system design and development environment.	PPP/Supply Chain Risk Management Section LCSP
Interoperability	Interoperability may be a component of security in that it evaluates interfaces between systems – these interfaces may be internal or external	Programs are required to test and evaluate systems to ensure information technology interoperability requirements are achieved	Information Support Plan (ISP) SEP



Additional cybersecurity standards, system cyber survivability, and operational 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 a high-level 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 standards, system cyber survivability, and operational resilience 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, system cyber survivability, and operational 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 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 test ranges and contractor or government labs require scheduling well in advance. In some cases, the government may contract with the developer for a T&E infrastructure such as a systems integration and test lab that could be used for cybersecurity T&E. The CyWG may want to carefully plan and coordinate with the contractor to ensure that the contractor test infrastructure can also be accessed and used by the government for cybersecurity T&E, if required. See Appendix F and Appendix X4 to assist with identifying resources.

Develop the Initial Operational Test (OT) Evaluation Framework. For the OT Evaluation Framework, the TEMP includes measures for cybersecurity and operational resilience as part of OT 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 should 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 Phases 1 through 6.



Align DCO Capabilities to Support the RMF. Identify inherited controls provided by outsourced DCO providers. Step 6 of the RMF process, continuous monitoring, is supported through monitoring and detection capabilities provided under DCO requirements. A Defense in Depth strategy that accounts for monitoring and detection at the perimeter, network, endpoint, and data levels should be identified and tested for measures of effectiveness and measures of performance.



Plan and Schedule an MBCRA. An MBCRA, such as a CTT exercise, examines stated, implied, and essential cybersecurity, system cyber survivability and operational resilience requirements; the cybersecurity risks the system may face; and possible impacts on mission operations. See Appendix X3 for more information. Performing multiple MBCRAs throughout the development lifecycle can provide the Program Office with a more comprehensive risk assessment and can provide the AO with a greater level of confidence for administering an ATO.

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 answers to the questions below for every planned test phase including the planned test activities in each phase. Depending on the system's stage of life cycle development, 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 will the testing occur (range, labs, contractor facility, distributed, etc.)?
- Why is the testing planned (controls assessment, architecture assessment, adversarial assessment, CTT verification, vulnerability assessment, etc.)?
- When will the testing events occur (frequency if repeated), including MBCRA events?
- How will the testing be conducted (tools, infrastructure, resources, threat, etc.)?
- How will execution of cybersecurity test activities and events provide data for evaluations?
- How will remediated or mitigated vulnerabilities be retested to verify removal of the vulnerability?

- How will the evaluations provide decision makers with essential information about the cybersecurity, system cyber survivability, and operational resilience of the system?

The strategy should 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 cybersecurity T&E six-phase process.

4.4 Phase 1 Data Requirements

- List of cybersecurity standards, system cyber survivability and operational resilience requirements and other factors that influence cybersecurity testing
- Inclusion of cybersecurity T&E items within the prototype RFP and system development RFP: Who, what, where, when, why, and how for contractor required cybersecurity T&E. More information about contract cybersecurity T&E language is available 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 should 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, system cyber survivability, and operational 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 DEF and OEF as described above.
- Plans and schedule for cybersecurity test activities with integrated 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 primarily inform the following acquisition reviews and decisions:

- **MS A Risk Reduction Decision.** Provide input into prototype testing. Testers provide T&E inputs for each prototype developed. MBCRAs performed on prototypes are useful in evaluating cybersecurity risk and down-select. Use the criteria, issues, COIs, CTPs, measures of effectiveness, and measures of suitability developed for prototypes to define the strategy for contractor cybersecurity T&E.
- **Prototype Development Decision/Capability Development.** Evaluate prototypes, architectures, new technologies; demonstrate that prototypes meet mission needs in cyber-contested environments. Demonstrate that the new joint capability can meet mission needs in a cyber-contested environment.
- **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.
- **System Requirements Review (SRR).** Provide input into the requirements review for any identified gaps in cybersecurity standards, survivability or operational resilience requirements.

- **MS B RFP and Contract Award.** Provide input to the RFP that details required contractor cybersecurity T&E activities and government-contractor integrated cybersecurity testing. Ensure that the contractor is also taking the necessary protections and flow down of protections to secure the development environments and development tools. Provide input on contractor cybersecurity testing and flow down of cybersecurity testing requirements for supply chain risk identified areas. See Appendix B for additional cybersecurity T&E contract language considerations.
- **PDR.** Consider providing a preliminary DT&E analysis in support of the PDR based on any prototype or sub-component testing that has occurred and the testing planned to date. A DT&E analysis will likely be more thorough after completion of Phase 2.
- **CDD.** Assess if the cybersecurity, system cyber survivability, and operational resilience requirements are testable, measurable, and achievable in both the draft and final CDD.

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, known vulnerabilities, and to explain 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.

The cyber-attack surface analysis informs:

- System design and operation, to eliminate or mitigate identified architecture susceptibilities
- Risk and potential mission impact from cybersecurity threats
- Test scheduling and planning to evaluate risk and whether vulnerabilities are reachable and exploitable

Cyber-Attack Surface

The different points in a system architecture where an attacker could gain entry to compromise a system or steal information from the 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).

The CDT takes advantage of component subject matter expertise, key documentation, and other references when performing this phase and characterizes the cyber-attack surface in conjunction with the systems security engineering process. Automated tools that ingest MBSE designs can facilitate more efficient Phase 2 analyses. The process for Phase 2 is the same for all acquisition programs, and Appendix C provides guidance on tailoring.

Figure 5-1 shows Phase 2 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.

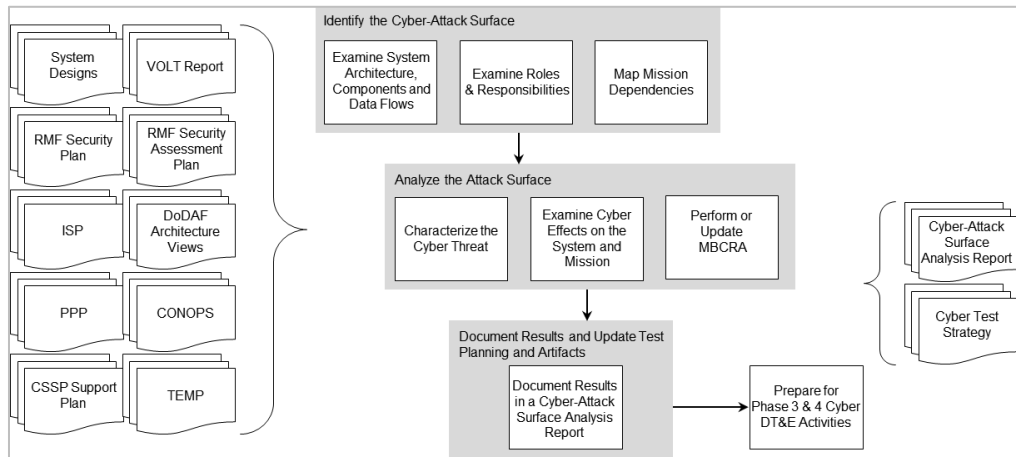


Figure 5-1. Phase 2: Characterize the Cyber-Attack Surface Activities

5.1 Schedule

Phase 2 ideally starts before engineering, manufacturing, and development (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. Phases 1 and 2 are essential for understanding what to test and how test and therefore should not be skipped! Phase 2 analysis is an iterative process as shown in Figure 5-2; Program Offices revisit this

phase before a major milestone, as part of an MBCRA, prior to test plan development for specific tests, or for any changes to the system’s attack surface or threat profile. The system’s attack surface can change in several ways. For example, a new vulnerability is discovered within Windows and the system uses that version; this should trigger an MBCRA. An example of a change in threat profile could be new intelligence collected for a certain location to which the system will eventually be deployed. 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.

Attack surfaces change throughout the development and testing cycles. Once ACD assessments begin, additional and more likely attack vectors and vulnerabilities may be 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.

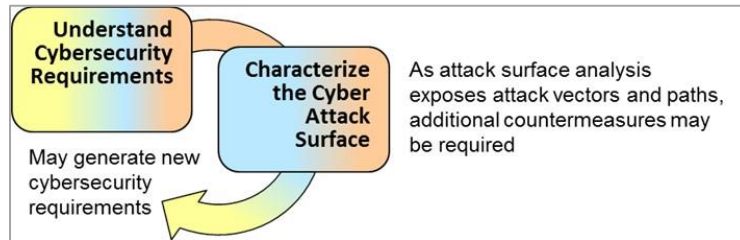


Figure 5-2. Phase 2 Iteration

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 standards, system cyber survivability, and operational resilience requirements assembled in Phase 1:

- Cybersecurity requirements and requirements traceability documentation
- CSRC
- CONOPS, Concept of Employment (CONEMP), User manuals
- Joint Mission Essential Task List for Joint Missions or Service-specific Mission Essential Task List
- Joint Common System Function List for Joint Missions⁷
- DBS Capability Implementation Plan
- DBS Capability Support Plan (if available)
- CSSP support plan
- Information Support Plan (ISP)
- LCSP
- DoDAF operational views (OVs), system views (SVs) and Data and Information View (DIV) points (DIVs) or MBSE artifacts:
 - OV-1: High-Level Operational Concept and other operational views as needed
 - SV-1: Systems Interface Description

⁷ Joint Staff J-6, Warfighting Mission Area, Architecture Federation and Integration Project Portal, (U) Joint Common System Function List (JCSFL). <https://wmaafip.csd.disa.mil/Project?&aId=54>. (14 August 2018)

- SV-2: Systems Resource Flow Description
- SV-6: Systems Resource Flow Matrix
- DIV-1: Conceptual Data Model (addresses the information concepts at a high-level on an operational architecture)
- DIV-2: Logical Data Model (allows analysis of an architecture’s data without consideration of implementation specific or product specific issues)
- DIV-3: Physical Data Model (describes how the information in DIV2 is implemented. Outlines data exchanges/interoperability risk reduction)
- 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
- List of critical components including detail for all logic-bearing devices to the component level and information necessary to conduct threat assessments of critical item suppliers
- 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
 - Supply chain illumination
- 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
- MBCRA



5.3 Tasks

The CyWG performs the tasks identified for Phase 2. Automated tools can simplify these efforts and support more frequent analyses.

5.3.1 Identify the Cyber-Attack Surface

Examine System Architecture, Components, and Data Flows. To characterize the cyber-attack surface, the CyWG first identifies all forms of communication, network connectivity, software, hardware, supply chain, 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 (MEFs). These are not the only potential attack surfaces but are the known attack vectors.



Security Standards: The RMF Security Plan and systems security engineering efforts examine the system architecture and may provide information on the cyber-attack surface. RMF controls are applied to protect the system from cyber threats but may inadvertently expand the system’s attack surface.

DCO monitoring and detection tools should also be identified within the attack surface. Will malicious activity be detected or not? 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 5-1. Mobile Navigation System (Notional) Attack Surface List

System Component	Interfaces	Information Exchanges	Data
GPS Receiver	<ul style="list-style-type: none"> • GPS antenna • Fiber interface • Serial port 	<ul style="list-style-type: none"> • GPS navigation messages (GPS antenna) • Navigation messages (Decryption module) • Configuration updates (factory) 	<ul style="list-style-type: none"> • Navigation data (encrypted, in transit) • Configuration data (at rest)
Decryption Module	<ul style="list-style-type: none"> • Fiber interface • Ethernet interface • Serial interface 	<ul style="list-style-type: none"> • Navigation messages (GPS receiver) • Navigation messages (Processing module) • Key management information (Key custodian) • System administration commands (Admin) 	<ul style="list-style-type: none"> • Navigation data (decrypted, in transit) • Cryptographic algorithm (at rest) • Cryptographic keys (at rest)
Processing Module	<ul style="list-style-type: none"> • Ethernet interface • Serial interface 	<ul style="list-style-type: none"> • Navigation messages (Decryption module) • Enriched mission information (Geolocation tagging unit) • Navigation messages (Geolocation tagging unit) • Storage information (Storage module) 	<ul style="list-style-type: none"> • Navigation data (at rest) • Maps (at rest) • Enrichment data (at rest) • Mission data (at rest)
Storage Module	<ul style="list-style-type: none"> • Ethernet interface • Removable media drive 	<ul style="list-style-type: none"> • Storage information (Processing module) • Archive download (Analyst) • Maintenance commands (Database manager) 	<ul style="list-style-type: none"> • Navigation data (at rest) • Mission data (at rest)
Geolocation Tagging Unit	<ul style="list-style-type: none"> • Ethernet interface • Fiber interface 	<ul style="list-style-type: none"> • Enriched mission information (Processing module) • Navigation messages (Processing module) • Mission and navigation information (Platform) • Mission and navigation information (Encryption module) • Maintenance commands (admin) 	<ul style="list-style-type: none"> • Navigation data (at rest) • Mission data (at rest) • Access control information (at rest)
Network Switch	<ul style="list-style-type: none"> • Ethernet interface • Wireless interface 	<ul style="list-style-type: none"> • Configuration updates (admin) 	<ul style="list-style-type: none"> • Navigation data (in transit) • Mission data (in transit) • Configuration data (at rest)
Encryption Module	<ul style="list-style-type: none"> • Fiber interface • Serial port 	<ul style="list-style-type: none"> • Navigation and navigation messages (Geolocation tagging unit) • Navigation and mission information (Radio Frequency (RF) transmitter) • System administration commands (Admin) 	<ul style="list-style-type: none"> • Navigation data (encrypted, in transit) • Mission data (encrypted, in transit) • Cryptographic algorithm (at rest) • Cryptographic keys (at rest)
RF Transmitter	<ul style="list-style-type: none"> • Fiber interface • RF antenna 	<ul style="list-style-type: none"> • Navigation and mission information (Encryption module) • Navigation and mission information (Command and control system) 	<ul style="list-style-type: none"> • Navigation data (encrypted, in transit) • Mission data (encrypted, in transit)

System Component	Interfaces	Information Exchanges	Data
Supply Chain	<ul style="list-style-type: none"> Media containing software updates Website for downloading firmware updates 	<ul style="list-style-type: none"> Maintenance port used to install software and firmware updates 	<ul style="list-style-type: none"> Corrupted system software or firmware with malicious code

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. This can also include support equipment allocated to the system such as an aircraft test kit, or maintenance laptop.
- Examine and include interfaces that are used as well as those not used for normal system functionality (i.e. maintenance port).
- 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 conducted a FMECA for the system, the data can supplement system design information as well as inform the cyber-attack terrain for a system.
- Understand the planned maintenance processes and human interactions including CSSP and DCO activities.



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
- 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 as well as 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. The mission should be decomposed down to the specific applications, functions within those applications, line replaceable units, and third-party libraries needed for the mission.

Key Cyber Terrain

Key Cyber Terrain or **mission-critical nodes** are the cyber components in a program associated with critical mission functions. The PPP mission-critical components in the criticality analysis section assists with identifying key cyber terrain.

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. The result can illuminate interdependencies of critical functionality on non-critical components and therefore identify additional areas in the supply chain that had not previously been considered critical. This mission decomposition, shown in Figure 5-3, will help in the next task, Analyze the Attack Surface.

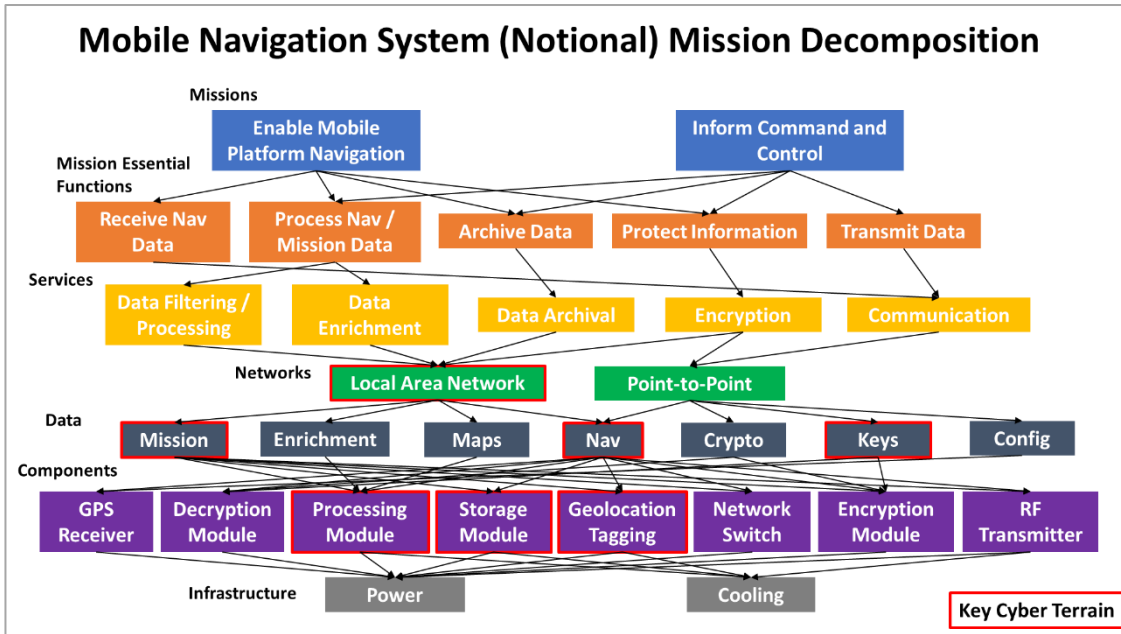


Figure 5-3. Example Mission Decomposition and Criticality Analysis

The result could be represented as a criticality overlay on the mission decomposition and attack surface list to use in the next task. The overlay would clearly identify in the attack surface list:

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

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, designed-in dependencies, 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.

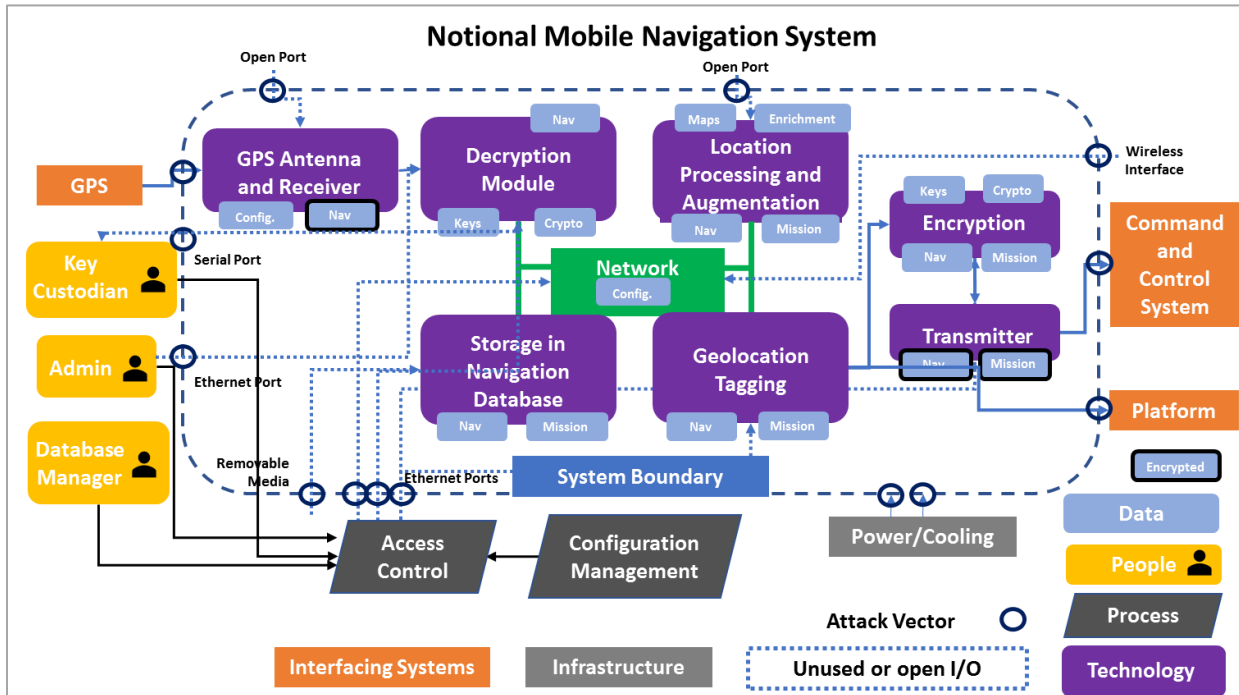


Figure 5-4. Example Cyber-Attack Surface System Diagram

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 testing in the next cybersecurity T&E phase or event within a phase (test events during Phases 3, 4, 5 or 6). 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 SP 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.

For system cybersecurity standards, the attack surface analysis should consider the following questions:

- RMF – How do the various controls (access controls, policy controls, configuration management controls, environmental controls, etc.) affect the attack surface?
- DCO – Are there detection capabilities for identified attack vectors? Does the system address continuous monitoring from a DCO perspective? Does the DCO capability make the system more



vulnerable by extending the attack surface? What are the vulnerabilities in the data correlation and analysis capability that may prevent effective cyber defense?

For system cyber survivability requirements, the attack surface analysis should consider the following questions:

- What are the impacts to system performance thresholds that could be disrupted during cyber-attack?
- Which of the mission critical systems are most vulnerable to an insider threat attack? Will the system detect an insider threat? What are the security measures in place (physical or logical) to reduce the risk of such a threat?
- What specific systems must operate in a degraded state to support mission operations? How long must they operate? This informs test planning focus on mission critical components and their recoverability to support mission execution.
- What specific systems must be recoverable to support mission operation? How long can system functions be inoperable before the mission is aborted?
- What specific threat (expressed as Adversary Threat Tier 1-4) is the system required to protect against?

For operational resilience requirements, attack surface analysis should examine the following questions:

- What is the fault-tolerance of the system?
- What systems or services are enabling system resilience that would extend the attack surface?
- What free and open source software (FOSS) or commercial off-the-shelf (COTS) products which cannot be tailored are included in the system?
- Does the system deploy deception techniques?
- How can the attack surface contribute to data loss and impact mission data integrity?
- What mechanisms exist to restore lost or damaged information resources to a trustworthy state while maintaining support to mission operations?

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 Tactics, Techniques 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 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

Characterizing the Cyber-Attack Surface

Perform an MBCRA to analyze the attack surface, examine the cybersecurity risks the system may face, and create a set of cybersecurity scenarios used for testing during upcoming test events. A CTT exercise is a useful tool for performing the MBCRA.

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 attack sequence phases. 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 system cyber survivability and operational resilience. 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. Additional frameworks to consider are the MITRE ATT&CK™⁸ model and the National Security Agency (NSA)/Central Security Service Technical Cyber Threat Framework⁹.

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, system cyber survivability, and operational 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 (NVD), 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.

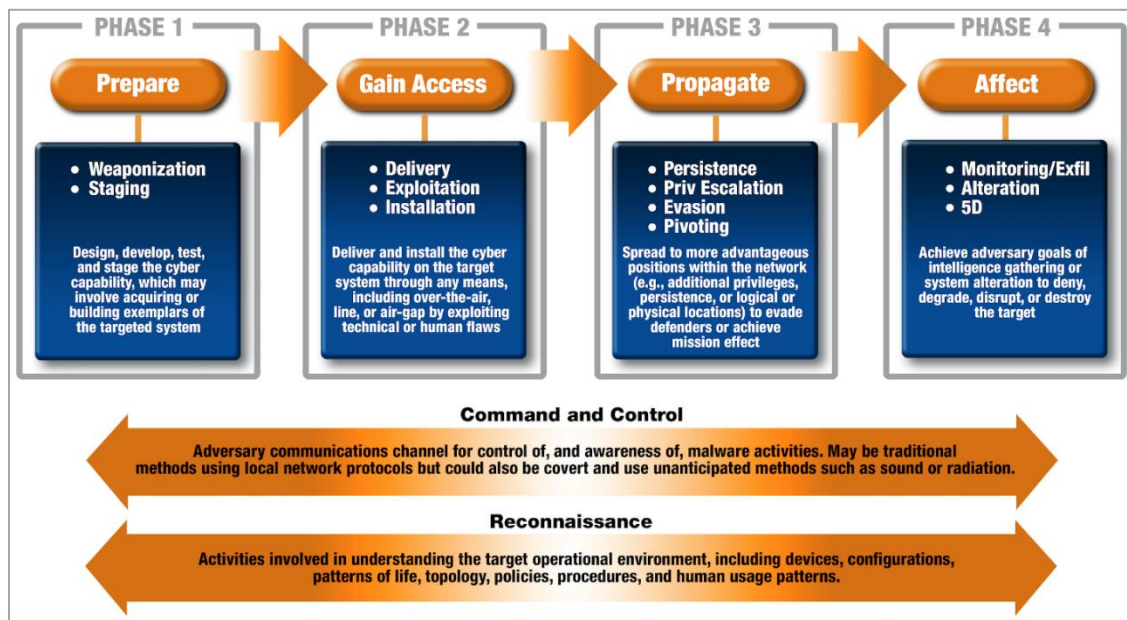


Figure 5-5. Cyber Kill Chain

⁸ https://attack.mitre.org/wiki/Main_Page

⁹ <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf>

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 one 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.

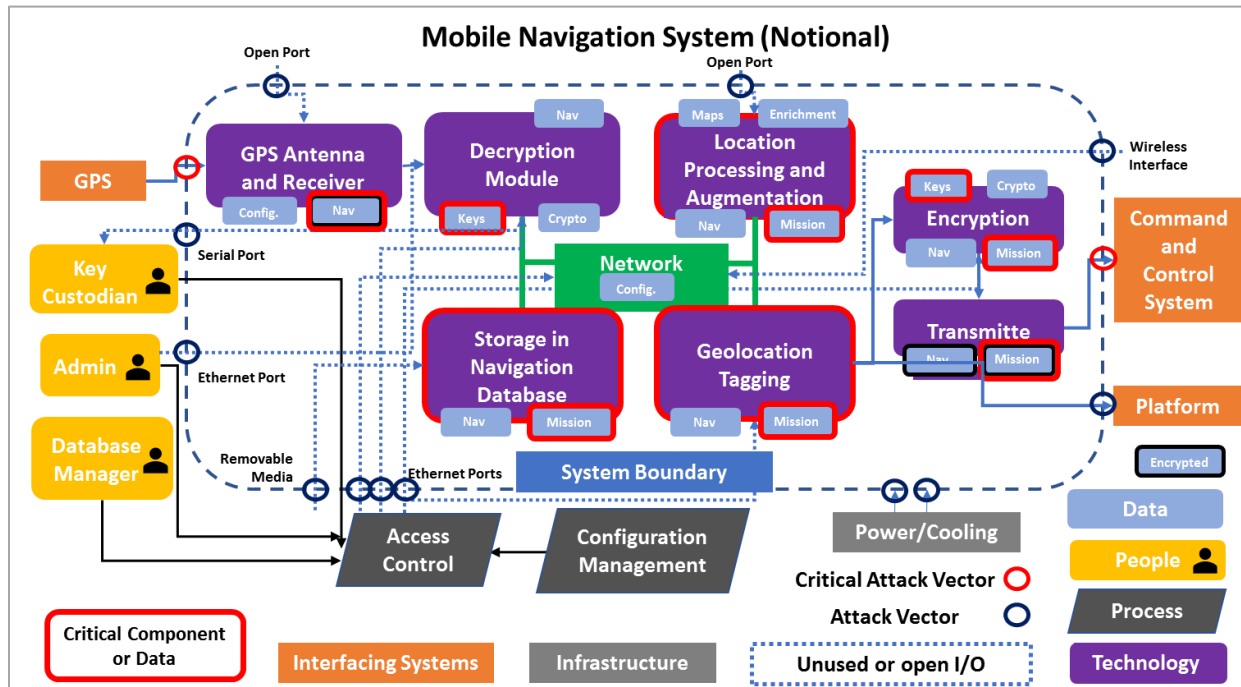


Figure 5-6. Example Attack Surface Analysis

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 MEFs to continue while a system is under attack. The CyWG should also document testing tools, infrastructures, and environments necessary to verify and validate cybersecurity, system cyber survivability, and operational resilience 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 MEFs, 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 cybersecurity, system cyber survivability, and operational resilience requirements. Note that the RMF process and systems security engineering efforts also examine the system architecture and may provide information for or be integrated with this analysis. The CyWG shares the report and all supporting documentation with SE, the Program Office, CDT, cybersecurity testers, and stakeholders.



Develop threat vignettes (use cases) to guide test planning. The results of attack surface analysis may be used to develop threat vignettes. Threat vignettes are story boards or system use cases that feature postulated or known system vulnerabilities. They tell a story about how an attacker may use a system vulnerability to gain access to the system and cause an adverse mission effect. Threat vignettes can be used to develop test scenarios for Phase 4 adversarial testing based on suspected vulnerabilities and attack paths discovered during Phase 2 analysis. Threat vignettes can also be used to inform SSE architecture and design reviews. Figure 5.7 illustrates a threat vignette use case.

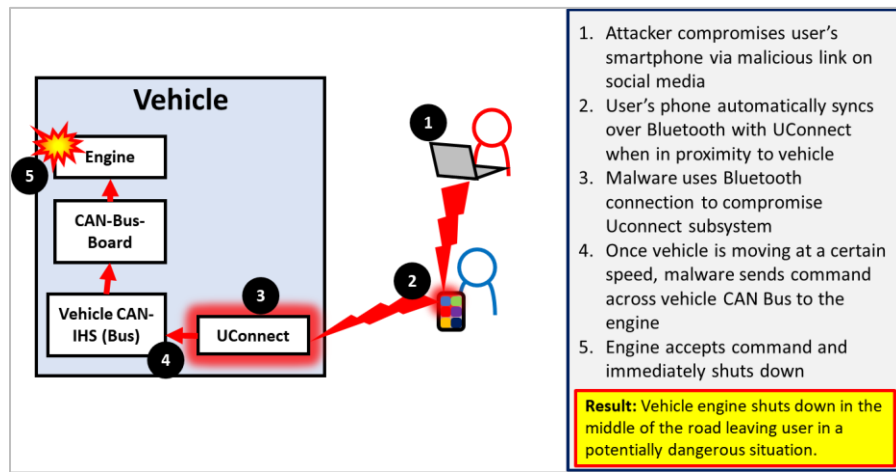


Figure 5-7. Threat Vignette Illustration

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. Contractor test activities should be planned as the first opportunity to perform Phases 3 and 4 activities with government DT&E and OT&E integration. The government testers can provide sanitized, relevant threat information as well as specialized test tools.

Formulate Test Strategy. The CyWG plans a series of Phase 3 and/or Phase 4 activities beginning with contractor (prototype or development) test, potentially as early as sub-component and sub-component

integration events, to 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 or data collection for interoperability certification
- 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
- DCO assessment to include Evaluators Scoring Metric maturity level, intrusion detection sensor testing, and CSSP incident response plan
- Supply chain testing



Schedule. The overall T&E schedule includes the ACD testing events for both contractor-government integrated testing prior to delivering the system to the government and government independent ACD; ACD assessment teams and infrastructures such as test ranges and labs require scheduling well in advance.

5.4 Phase 2 Data Requirements

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, potentially leading to a repeat of Phase 1. 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, those identified through the RMF process (as documented later in the RMF Plan of Action and Milestones [POA&M], if available) and through the Program Deficiency Reporting (DR) process
- 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 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, system cyber survivability, and operational 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 DCO, interface representation
 - Schedule
 - What contractor testing will be performed
 - Integrated testing
 - Risks associated with areas not planned for testing
- Updating DEF and OEFs

5.4.2 Acquisition Reviews and Decisions Informed by T&E

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

- **SRR.** Provide input into the requirements review for any mitigations for attack surface areas of concern (additional tailoring of controls, changes in procedures, supply chain concerns, etc.).
- **CDD Validation.** Assess whether the cybersecurity, system cyber survivability, and operational 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, system cyber survivability, and operational 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 the maturity of cybersecurity, system cyber survivability, and operational 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 and the cybersecurity test lead were then able to work with a cyber range to plan and develop a CVI Test event 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.”



6 Phase 3: Cooperative Vulnerability Identification

The CVI phase, which Enclosure 14 of DoDI 5000.02 and DoDI 5000.75 require, consists of detailed planning and execution of cyber 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. Contractor CVI activities should be planned during prototype and system development. The CDT evaluates contractor test data against SE-defined CTPs to validate that the system as operationally fielded meets the stated capabilities. The vulnerability assessment team assesses vulnerabilities and provides feedback to system developers and engineers to resolve discovered vulnerabilities. The vulnerability assessment team also performs cooperative penetration testing to demonstrate exploitability of identified vulnerabilities and improve system cyber survivability and operational resilience. CVI testing can be used to tune and train DCO systems during cooperative penetration test events. Phase 3 activities are cooperative in that the attack surface documented during Phase 2 informs the Phase 3 vulnerability assessment team efforts and Phase 4 adversarial test 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.

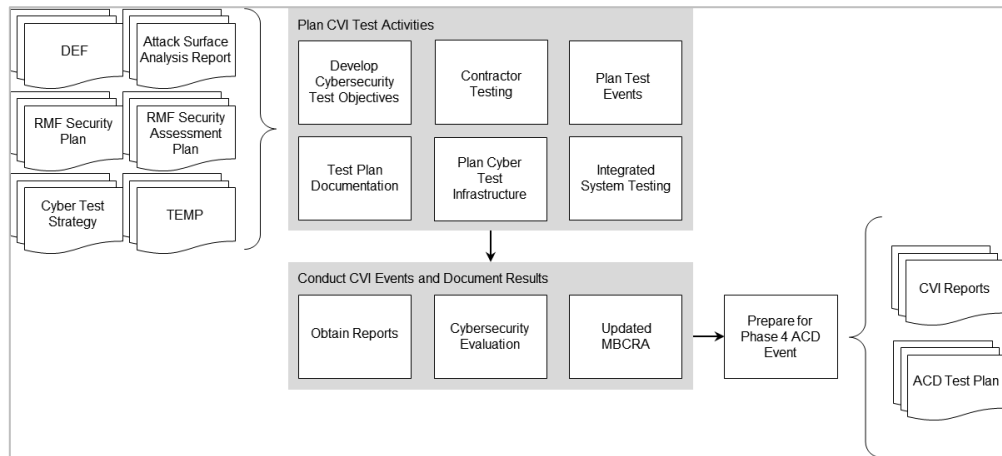


Figure 6-1. Phase 3. Cooperative Vulnerability Identification Activities

CVI is not a single test event. The CDT and the contractor should plan and conduct test activities designed to test, analyze, fix, and retest the prototypes, components, subsystems and systems throughout integration and 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 contractor or government cybersecurity evaluation (test report) that assesses the status of all discovered vulnerabilities (remediated and/or mitigated), current and anticipated threats, and risks to mission operations.

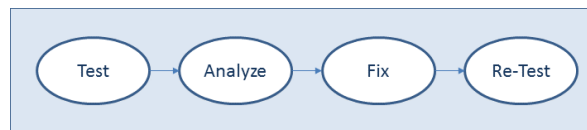


Figure 6-2. Phase 3 Testing Process

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 RMF Security Plan. CVI results may include SCA results for the IATT request. When



possible, CVI should include cooperative penetration testing. In a cooperative penetration test, testers simulate an attacker by using tools and methods an attacker is likely to employ while attempting to circumvent the security features of the system.¹⁰ The intent is to evaluate exploitability of the vulnerabilities or exposures.

Phase 3 testing lays the foundation for successful Phase 4 ACD by identifying known exploitable 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, NVD and CAPEC (see References). CVI testing verifies exploitability in the tested component or system and should include mitigations, if possible, of known component and software vulnerabilities. Phase 4 will later evaluate the mission effects of the remaining exploitable vulnerabilities or exposures and may identify previously unknown vulnerabilities, exposures or features that can cause mission impacts.

6.1 Schedule

CVI planning begins before MS B for acquisition programs under the DoDI 5000.02 or after the ATP decision for DBS under DoDI 5000.75. CVI testing should be planned and executed by the prototype contractors. The CDT documents the plan for prototype testing in the MS A TEMP and for system development in the MS B TEMP or the DBS implementation plan documentation and should ensure the RFP and resulting contracts include contractor planning, analysis and conducting a tailored series of cybersecurity T&E. CVI test execution should begin as early as sub-components, components, integration of components and system maturity allows. Vulnerability testing results (mitigated, not able to be mitigated, not exploitable, and not mitigated) from CVI test events 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 should 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 exploitable vulnerabilities have been remediated by the contractor, if possible, or by other means, and verified as mitigated. The schedule should allow time for final verification of mitigation for mitigated vulnerabilities prior to Phase 4 ACD. For information on tailoring Phase 3, refer to Appendix C.

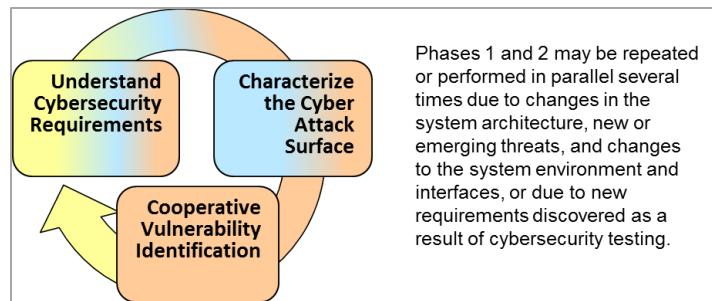


Figure 6-3. Phase 3 Iteration

6.2 Inputs

The following artifacts are inputs to Phase 3 and inputs when iterating Phase 3 after each test event or after iterating Phases 1 and 2. Appendix D further describes key artifacts for T&E analysis.

¹⁰ Office of the Chief Engineer (NAVWAR 5.0). Cybersecurity Technical Authority (CS TA) *Cyber Risk Assessment (CRA) Standard Volume 1: Cyber Vulnerability Discovery Guide*, 2019

- Cybersecurity portion of the DEF
- Attack Surface Analysis Report from Phase 2
- Test results from contractor T&E activities (prototypes, sub-components, integration testing)
- Test results from contractor Service/Component-level testing, testing integration of components
- Test results from contractor full system testing
- Verification of fixes reports
- Software Requirement Specification
- Software Test Plan and software assurance test results
- DBS Capability Implementation Plan
- DBS Capability Support Plan
- Test Strategy for Phase 3
- Updated TEMP
- RMF Security Assessment Plan
- RMF Security Plan
- CONOPS, CONEMP user documentation
- LCSP
- MBCRA (e.g., cyber table top) results



6.3 Tasks

The CDT has the lead role for cybersecurity test planning, execution, and reporting during Phase 3. The CDT should ensure the contract (for prototypes and for system development contracts) includes contractor cybersecurity test planning, reporting, mitigation of vulnerabilities, verification of mitigated vulnerabilities, reporting on vulnerabilities that were not or could not be mitigated, integration of government cybersecurity testers during contractor cybersecurity test planning, testing, and mitigation verification, and required cybersecurity testing of identified sub components, components, sub/component integration, and full system integration. The contract should address supply chain flow down requirements for cybersecurity testing, contractor verification of supply chain cybersecurity testing (software, hardware, sub components, components, etc.) as specified by Phase 1 and 2 analyses. If CVI is being combined with a CVPA, the OTA is responsible for planning, conducting, and reporting the CVPA activities.

6.3.1 Plan CVI Test Activities

The CDT and CyWG, including the vulnerability assessment team and adversarial DT&E and OT&E 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 cyber survivability and operational resilience. 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. Initial testing will not necessarily be in a mission context and should address all functionality of a sub-component and component to identify new exposures and features.

Develop Cybersecurity Test Objectives. The CyWG develops cybersecurity test objectives to guide test planning and align with the CTPs. Test objectives describe the desired outcomes from test activities, along with measures that demonstrate improvement as SUT development progresses. Test objectives

should be defined for standards, system cyber survivability and operational resilience. As discussed in Section 3.7, some objectives may overlap all three areas, two areas, or be unique to the area of focus. An important goal of test planning is to design tests that produce repeatable, defensible test results that effectively support decision makers. Test instrumentation, data collection efforts, and applying 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. Test objectives are necessary inputs to planning instrumentation, data collection and applying STAT. For more information on STAT, see the DAG, Chapter 8-3.7.4.

Testing Security Standards. Phase 3 includes verification of DoD policy requirements levied on various technologies, data types, capabilities, and systems that if not followed may introduce vulnerabilities. Each program should identify the components within their own system that may have required standards. Examples of technologies, data types, capabilities, and systems with DoD policy mandated standards:

- Development environment
- DoD internet services
- Approved Product List
- Biometrics
- Cross Domain Services
- Mission Partners data sharing
- Public Key Infrastructure
- Health Systems
- Space Systems
- Communication Security, includes encryption
- Identity access management, credential strength

RMF - Phase 3 testing includes the contractor system development testing of the RMF controls. CDTs and system test leads should also verify security controls through testing once the SUT or new capability is delivered to the Program Office. Controls testing also provides feedback to the SE on the effectiveness of the security design and informs the IATT and ATO.



DCO - Phase 3 testing includes contractor and the CDT evaluation of the people (planned roles), processes, and technologies enabling DCO activities to prevent, mitigate, and recover from cyber-attacks. When conducting a cooperative penetration test during CVI events, the DCO capabilities should be included or emulated to the maximum extent possible.

DCO test objectives should be developed that test the system's protection, detection, and response capabilities. Example DCO test objectives include:

- Verifying the system's protection and detection mechanisms, such as detecting unauthorized access and abnormal usage patterns
- Sensor testing: What abnormal system activity can be detected and what cannot be detected
- Verifying the response producers
- Verifying the system fully recovers required mission-critical functions and system recovery falls within acceptable mission performance thresholds

A cooperative test event provides the only opportunity to test and hone the DCO capabilities against a known cyber-attack, even if not detected. In non-cooperative test events, the security operation center (SOC) operators must first determine whether they are experiencing a cyber-attack, a maintenance issue, or just an anomaly based on their personal experience. Including DCO capabilities in cooperative penetration testing is an excellent way to:

- Maximize tuning and signature creation of the tools for effective detection
- Establishes a baseline of normal versus anomalous activity

- Provide operators/technicians experience recognizing cyber-attacks.

At the conclusion of the test event, in addition to the penetration team’s outbrief, the DCO team should also provide an assessment or report that includes discovered vulnerabilities lessons learned, and constraints.

Testing Operational Resilience. During Phase 3, components of the SUT and the SUT itself should be tested starting from a non-operational or degraded state to test restoring lost or damaged information resources. Develop test objectives to examine restoration to a trusted state within the thresholds required for mission operations. The vulnerability assessment team uses cooperative penetration testing to demonstrate and improve operational resilience and to demonstrate that system functions can continue to support mission operations.

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
- Safety aspects of the system that could be impacted by a cyber threat



Testing System Cyber Survivability. Cybersecurity testing during Phase 3 also includes assessing the CSAs and evaluating the CSRP after each test event. Table 6-1 shows example program test objectives, technical test objectives, and metrics based on CSE IG system CSAs supporting an assessment of PMR. PMs should test the system CSAs associated with PMR during CVI and assess PMR including DCO capabilities during Phase 4. CDTs and system test leads should tailor the test objectives based on the CSAs applicable to the SUT.

Table 6-1. Example Program Test Objectives, Technical Test Objectives and Metrics

Example Program Test Objectives	PMR/CSA	Example Technical Test Objectives	Example Metrics
System monitors the cybersecurity configuration baseline for cyber anomalies in real time by: <ul style="list-style-type: none"> • Performing malicious code protection; • Intrusion detection using automated tools for real-time analysis; • Information system monitoring; • Security alerts; • Security function verification; • Software, firmware, and information integrity; • Incident monitoring, handling, reporting, and response 	<p>Prevent CSA 3: Reliable, Confidential Transmissions and Communications CSA 4: Protect System’s information from exploitation</p> <p>Mitigate CSA 7: Monitor System and Detect Anomalies</p>	Determine the system’s susceptibility to cyber-attacks. Examine integrity and confidentiality of critical-mission data. Ensure cryptographic devices are operating as intended.	Percent of malicious code detected in tested software. No unauthorized software is resident on operational system.
System detects and discards malformed messages and invalid inputs.	<p>Prevent CSA 4: Protect System’s information from exploitation</p>	Verify: System validates data inputs for mission related data.	Percent of tested malformed and invalid inputs blocked/dropped.

Example Program Test Objectives	PMR/CSA	Example Technical Test Objectives	Example Metrics
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.	Prevent CSA-1: Control Access CSA-4: Protect System’s information from exploitation	Verify: Access control denies access to unauthorized connections and user/process interactions Unauthorized attempts are identified and denied Effectiveness of internal and external boundary defenses.	Percent of tested unauthorized access attempts are deflected.
System degrades gracefully (e.g., quality of service) before degrading to unacceptable mission consequences	Mitigate CSA-8: Manage System Performance if degraded by cyber events	Verify: System maintains minimum performance required to prevent adverse mission consequences.	System degradation falls within acceptable mission performance thresholds.
System recovers mission-critical functions to enable mission completion.	Recover CSA 9: Recover System Capabilities	Verify: System fully recovers required mission-critical functions.	System recovery falls within acceptable mission performance thresholds.
Software patches and updates are authenticated using digital signatures and vendor-approved techniques.	Mitigate CSA 10: Manage System Patches and Vulnerabilities	Verify: Patch process authenticates all software patches and system updates prior to initiating the patching process.	Percent software patches and system updates authenticated before patch initiation.
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.	Mitigate CSA 10: Manage System Patches and Vulnerabilities	Verify: Patch and vulnerability management effectiveness, including timeliness for pending patches and critical patches.	Percent of critical patches deployed within the required timeframe.

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 test events to ensure that the vulnerability assessment teams have all the levels of system access required to 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. In addition, as software updates are applied to the system, the CDT plans to evaluate for newly introduced vulnerabilities, default configuration impacts, and other complexities that can result from updates.

The CDT plans for a continuum of CVI activities scheduled throughout prototyping and development. Overall prototype cybersecurity testing (CVI and ACD) is planned rather than a set of test events during prototype development. The prototype contract must inform the prototype contractors of the government cybersecurity testing requirements. Early in system development, CVI testing focuses on software, hardware sub-components, integrated sub-components, sub-systems and components that the contractor performs. CVI activities include contractor cybersecurity T&E activities during Phase 3 starting at MS B. The earliest developmental test activities, except for prototypes, are contractor T&E activities supporting

contractor development efforts and are optimized when the government and contractor are integrated for cybersecurity tests. The scope of contractor cybersecurity test activities informs the later scope of government independent cybersecurity T&E activities. Government testers should 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 prototype and development RFPs 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 components and platforms, the CDT should plan testing events to conduct CVI across interfaces (gathering interoperability data and interoperability certification data), with emphasis on critical data exchanges and interfacing systems with critical mission impact. Testing should continue until a full-up system is completely tested by the contractor, to include Phase 4 by the contractor, and eventually by the government as well.

Later developmental testing also includes cooperative penetration testing. Penetration testing is important in contrast to vulnerability testing. Penetration testing involves exploiting groups of vulnerabilities to gain more access than could be achieved through a single vulnerability.¹¹ Later in development, prior to government independent 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 resilience to cyber-attacks. The Program Office should track vulnerabilities and mitigation efforts. Ideally, the contract language will support the contractor requirement to mitigate any government identified mission-impacting vulnerabilities. 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 6-2 below describes examples of various developmental vulnerability test activities to plan and conduct during CVI by both the contractor and the government. The CDT tailors and selects tests that align with system test data requirements, attack surface, and critical functionality including vulnerability test activities in the developer’s contract.

Table 6-2. Example Test Activities

CVI Test Activities	Description	Test Conductors	Test Considerations
Architectural Vulnerability Assessment (AVA)	Examines network and system architecture attributes that may introduce attack paths to critical cyber assets.	System architect, system security engineer	Examine contractor technical design documentation. Investigate inherent architectural vulnerabilities. Examine trust relationships external to the SUT and critical data exchanges.

¹¹ Office of the Chief Engineer (NAVWAR 5.0). Cybersecurity Technical Authority (CS TA), *Cyber Risk Assessment (CRA) Standard Volume 1: Cyber Vulnerability Discovery Guide*, 2019

CVI Test Activities	Description	Test Conductors	Test Considerations
Software Testing	Identifies and eliminates software errors and vulnerabilities in critical components; contractor T&E is the earliest instance of software testing.	Contractor software tester Government software tester	Perform software security verification using requirements specified in the PPP. Address three areas: <ul style="list-style-type: none"> • Software development environment • Software development processes • SUT operational software For more information, see Appendix G.
Network Vulnerability Assessment	Targets SUT’s enclave network boundary, internal networks, system interfaces, and network security components.	Government network engineer	Test for misconfigured devices and nonfunctional protections at the network level, such as network segmentation and firewalling.
RMF Control Verification	Verifies cybersecurity functionality to ensure that security controls and countermeasures are working as intended in a mission context.	Security controls assessor Cybersecurity tester	Test security controls and countermeasures in a mission context before IATT. Verify contractor cybersecurity T&E results. 
Platform and Component Hardening Verification	Verifies security of components and platforms at the supply chain and hardware levels.	Vulnerability tester	Platform and component hardening verification provides input to the SE process. Assess patching processes for components to address vulnerabilities that occur after deployment. Assess Anti-Tamper (AT) measures.
Developmental STIG Verification	Rigorous component scanning that includes evaluating scan results, eliminating false positives, and performing manual checks.	Vulnerability tester	Test each critical cybersecurity asset and adjudicate all confirmed findings. Use multiple scanning tools to cross-validate vulnerability findings. Note: STIG verification during DT&E provides input to AO and does not replace RMF SCA. 
CTT Exercise Verification Test	Provides actionable information to PMs about mission impact of vulnerabilities discovered during CTT exercises.	CTT exercise Opposing Force team	Test suspected exploitable vulnerabilities to validate CTT exercise findings. Evaluate system performance during cyber-attack using safe test environments.

CVI Test Activities	Description	Test Conductors	Test Considerations
System Misuse/Abuse Testing	Examines how systems are used that are unplanned, unintended or unexpected.	Government penetration testers	Use misuse/abuse scenarios to guide testing with a mission context. An understanding of predicted cybersecurity threats provides input into system abuse scenarios.
System Cyber Survivability Testing	Ensures that the system can survive cyber-attacks to enable mission execution.	Government security testers	Refer to the CSE IG for more information. ¹²
Penetration Testing	Authorized, simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system’s features and data.	Penetration testers and adversarial testers	Target key cybersecurity and operational resilience assets supporting mission-essential functions for penetration and exploitation.
Cyber-EW Testing	Cyber-EW implications of new, existing or modified waveforms on mission operations.	Test engineers specializing in EW impacts to cyber components and cyber-attacks across radio frequency (RF) spectrum	Testing should consider waveforms and RF apertures as cybersecurity threat vectors.
Testing Non-IP Devices	Verify security of embedded systems and platforms at the supply chain and hardware levels.	Test engineers specializing in Supervisory Control and Data Acquisition (SCADA) systems, 1553 bus, Controller Area Network (CAN) bus testing	Appendix X5 discusses considerations for testing embedded systems and non-IP devices.

Test Plan Documentation. The TEMP documents planned tests. The test organization (contractor or government tester) develops detailed test plans for each test event. 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. An example outline for a test plan is shown below.

¹² *Cyber Survivability Endorsement Implementation Guide (CSE IG) v2.03*, Joint Staff/J6, Deputy DoD Chief Information Officer (CIO) for Cybersecurity, Defense Intelligence Agency (DIA), and the National Security Agency.

Example Test and Assessment Plan Outline

Chapter 1: Introduction

- Program objective of testing
- System Description
- External Connections
- Supply Chain Description

Chapter 2: Assessment Management

- Roles and Responsibilities – both operational roles and assessment roles
- Entrance Criteria for the test
- Event Dates, Schedule, and Locations
- Test Requirements and Required Resources
 - Test Articles
 - Funding
 - Personnel
 - On-Site Accommodations
 - Connectivity and Network Connections
 - Special Training Requirements
 - Test Limitations and Special Cases

Chapter 3: Assessment Execution

- Scope of the Assessment - Define the major activities of the test strategy and how testing will flow to meet test objectives
- Required Documentation and Artifacts Assessment
- Technical Controls Assessment
- Methodology and Approach – Describe:
 - Cyber Threat Representation
 - Data Handling
 - Event Preparation
 - System Operation
 - Vulnerability Assessment, Penetration Testing (PT) to be performed
 - Specialized testing (such as non-IP based, embedded system testing)
 - Mitigation Plan – how will vulnerabilities be fixed and retested?
 - Assessment Tools

Chapter 4: System Architecture

- Document the system configuration that will be tested
- Describe the cyber test techniques that will be used for the assessment that are specific to the SUT
 - Operational systems to be tested
 - Maintenance ports
 - Network testing
 - Embedded system testing
 - Software testing

Chapter 5: Conclusions

Chapter 6: References, List of Symbols, Abbreviations, and Acronyms

The planned testing activities, such as the examples in Table 6-2, dictate the expectations for the knowledge, skills and abilities of the tester. Vulnerability testing requires a high degree of expertise in a wide variety of disciplines to maximize the number of vulnerabilities discovered and minimize the number of false positives. Team members should be augmented by SMEs very familiar with the physical,

architectural, and environmental constraints of the system under test.¹³ These experts may have cybersecurity specialized expertise or may be technology SMEs (mobile device, commercial cloud hacker, software defined radio, AT, etc.) Often, these SMEs are a high-demand, low density asset. Therefore, the CyWG should ensure the SMEs can participate in the Phase 1 and 2 activities, MBCRAs, test plan development, and test events. Use Appendix F to help select the appropriate test resources for the various planned test activities.

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 and contractor plan and schedule cybersecurity test infrastructure to support test events and test data needed to resolve test objectives and ensure the use of contractor test facilities for early DT&E activities is documented in the contract. 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

DT&E Test Activities	Test Facilities	Example Cyber Test Activities
Hardware and Software Development Test	Contractor or government system development labs	Phase 3 – Hardware and Software Development Testing
Component and Subsystem Test	Contractor or government system integration labs	Phase 3 – Platform and Component Hardening
System Integration Test	Contractor or government system integration labs	Phase 3 – Cyber Functional Verification, Vulnerability Assessments
Operationally Relevant Test	Government hardware-in-the-loop (HWIL) facilities, cyber ranges	Phase 4 –ACD, CTT Verification Testing

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.

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?

¹³ Office of the Chief Engineer (NAVWAR 5.0). Cybersecurity Technical Authority (CS TA) *Cyber Risk Assessment (CRA) Standard Volume 1: Cyber Vulnerability Discovery Guide*, 2019

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. Baseline 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.

Scoping Testing

Use an MBCRA/CTT to conduct cyber kill chain analysis to determine potential cyber-attacks, impacts, and mitigations prior to testing to focus and prioritize limited testing resources.

6.3.2 Conduct CVI Events and Document Results

Vulnerability assessment teams (contractor, government, or integrated contractor-government teams) conduct CVI test events, which include government prototype cybersecurity test activities, and contractor and government cybersecurity test activities between MS B and MS C. The CDT provides all 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 (or other tool) 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 to determine potential cyber-attacks, impacts, and mitigations. CVI reports describe results of CVI analysis, recommended corrective actions for the system, and corrective actions that may be deferred.



Evaluate Cybersecurity. Cybersecurity testing during CVI is a risk reduction activity that results in a cybersecurity evaluation of the data and test results. The evaluation may inform DCO support plans, LCSP, or updates to system requirements. The evaluation should address the CSRP. Section 3.8.1 discusses cybersecurity evaluations.

Update MBCRA. 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 Events

The completion of Phase 3 includes finalizing infrastructure planning for the ACD event(s) performed in the next phase. For contractor Phase 3 and 4, the two phases should be repeated until delivery to the government for independent CVI and ACD events. 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?
- 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 a systems-of-systems context during Phase 4 testing. ACD assessment teams and infrastructures such as test ranges and labs require scheduling well in advance. The overall T&E schedule should include ACD testing events.

6.4 Phase 3 Data Requirements

- Details of test conduct: schedule, locations, test organizations, test articles, and any test limitations or constraints
- Description of the SUT and relevant interfaces for testing; system protection mechanisms application to the SUT; life cycle sustainment considerations
- Formal CVI reports documenting exploited vulnerabilities and system exposures and associated cybersecurity evaluations
- Cybersecurity evaluation to include assessing the CSRP
- Evidence that known system vulnerabilities are either remediated or enumerated and tracked; remaining vulnerabilities are disclosed to adversarial test team for Phase 4 ACD
- 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 identifies and explains the incorporation of specific CVI test events into overall test planning. The TEMP should 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 test articles and government resources required to complete cybersecurity testing, including cybersecurity and technology specific SMEs, specialized test tools or connections, data collection and instrumentation needs, 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 the maturity of cybersecurity, system cyber survivability, and operational 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, system cyber survivability and operational resilience evaluations will inform each limited deployment ATP for DBS under DoDI 5000.75.
- **TRR.** Mitigation status to include verification of fixes or inability to mitigate vulnerabilities.

- **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.”

7 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 cyber survivability and operational resilience 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 cyber survivability and operational resilience. ACD should be performed by the contractor, with integrated government testers, before delivering the system to the government for government DT&E.

The goal of ACD is to verify system cyber survivability and operational resilience requirements and discover previously unknown, critical vulnerabilities and determine the mission impact of all vulnerabilities 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 cyber survivability and operational resilience to cyber-attack.

It is important to revisit Phases 1 and 2 before proceeding into ACD execution. By verifying the cybersecurity, system cyber survivability and operational resilience requirements and re-analyzing the attack surface terrain, the test team will be able to focus their testing on the part of the system that needs further verification. 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 not required. The contractor should be expected to 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.

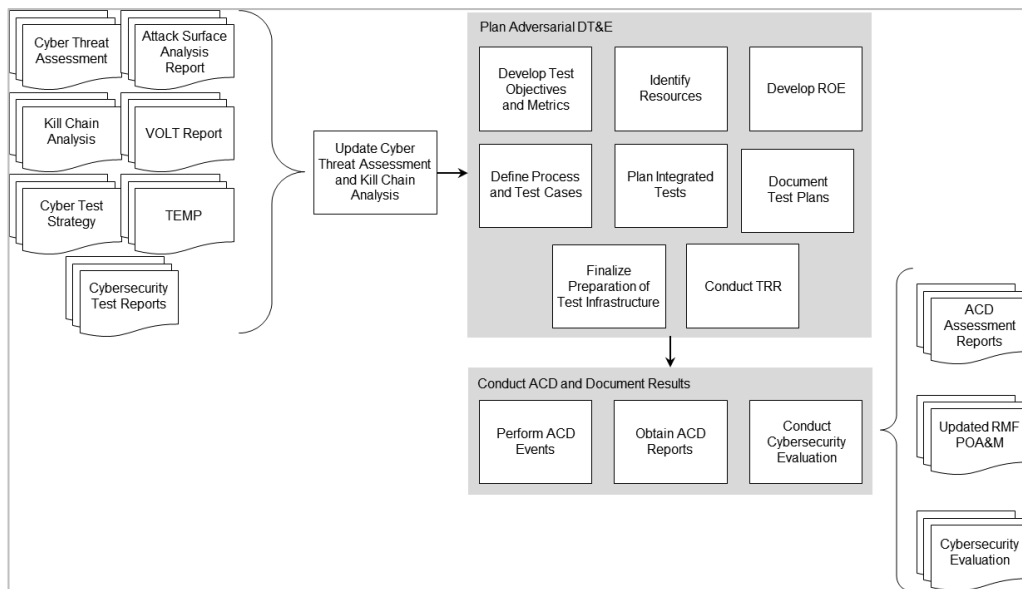


Figure 7-1. Phase 4: Adversarial Cybersecurity DT&E Activities

7.1 Schedule

The CDT plans for this phase during initial Phases 1 and 2, documents the planned events in the integrated test schedule and TEMP, and refines the plan and schedule as needed during Phase 3. The CDT plans to have the contractor conduct ACD events before delivery of the prototype or the developed system to the government for government cybersecurity DT&E. As part of significant functional releases, at least one ACD event should be planned prior to MS C and before the ATO to inform production and ATO decisions. CDTs should include contract language and 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 should 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:

- Cybersecurity requirements and requirements traceability documentation
- 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
- CSRP
- Mature and stable system baseline
- CONOPS, CONEMP, user documentation
- LCSP
- 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, specialized technical experts, as required, Red Teams, test planners, and test infrastructure planners. The typical 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. Government testers should be integrated with contractor testers to facilitate sharing sanitized or relevant threat information to support contractor ACD events. 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 test 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 operational resiliency in the face of validated cyber threats. One way to evaluate system cyber survivability and operational resilience 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 and prevent threat activity, mitigate the effects of threat activity, and recover mission capability degraded or lost due to threat activity. The preliminary assessment of PMR demonstrates how cyber survivable or resilient the system is in response to cyber-attacks and malicious activities.

Test Operational Resilience. To test operational resilience requirements during DT&E, testers should exercise the system's ability to recover MEFs, data and information within the parameters of mission requirements. For example, if a DoD mission system requires navigation data to reliably perform its mission CONOPS within 30 minutes of mission initiation, then navigation system components should have the ability to recover to meet the 30-minute requirements. CDTs and test leads should plan and conduct operational resilience testing consistent with DoDI 8500 Enclosure 3.

Test System Cyber Survivability. To test system cyber survivability requirements during DT&E, testers should exercise the system's ability to detect and prevent attacks, mitigate effects of system penetrations and exploitations, and ensure that the system is able to recover to a known trusted baseline to continue executing the mission.

Test Security Standards. RMF: During Phase 4, testing of operational resilience and system cyber survivability informs RMF controls compliance; RMF controls testing is not conducted during Phase 4. Following Phase 4 adversarial testing, test results inform the AO about mission-based cyber risk based on the results of operational resilience and system cyber survivability. Formal SCA should be conducted after completion of Phase 4 Cyber DT activities.



DCO: Phase 4 testing measures the effectiveness of the mitigation and recovery activities that follow a cyber-attack. Each test event involving DCO is an opportunity to better understand the digital environment during an attack. The results of each test event should be analyzed to determine if detection oversights were based on system configurations or just failure to be recognized. Phase 4 testing also measures the time to recovery and incident response effectiveness. Testing should include opportunities for additional network signatures to be added as needed in the face of an attack with the constraints levied by the configuration management process to fully understand the effects of response and recovery procedures during operations. 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.

Integrate Government Phase 4 and Phase 5. Phase 4 test can provide the opportunity for gathering data needed for Phase 5. Phase 4 and Phase 5 tests have separate test objectives, and the test plan should document these separate objectives.

Define Metrics. The CDT clearly defines the test data that needs to be collected during the ACD event that supports cybersecurity, system cyber survivability, and operational resilience measures. See Appendix X1 for considerations of cybersecurity measures for T&E. The CDT should ensure that test metrics are aligned to the test objectives and that the testing teams can collect 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 if unique or proprietary test infrastructure is needed for the program
- Using a test infrastructure that belongs to the contractor or other organization

Develop Rules of Engagement (ROE). For government ACD events, the PM and ACD assessment team develop and document the ROE and the scope of the assessment in the test plan before the event. This agreement may involve legal counsel and the 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 technical configuration settings and operator workflows to optimize cybersecurity, system cyber survivability and operational resilience defenses and include a limited test-fix-test methodology. Some identified vulnerabilities will require more significant changes to resolve, and the contract should include language that requires the contractor to correct or mitigate any government identified mission impacting issues. The CDT resolves deficiencies 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:

- Test objectives
- Test data that will be collected
- Data to be measured from any mission effects due to cyber compromise, and the party responsible for collecting those effects.
- Data collection processes and instrumentation
- 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

Section 6.3.1 provides an example of a cybersecurity test plan. For more information on test plans, see the DAG, Chapter 8-3.6.4.

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 for government ACD events as early as possible as early as possible 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 should also be involved in the test infrastructure planning.

As much as possible, the CDT plans to perform ACD events in an emulated DoDIN (if the system will interoperate with the DoDIN) in a separate enclave.

Any adversarial testing taking place on the DoDIN or traversing between the DoDIN and the internet will require an NSA-certified and U.S. Cyber Command (USCC)-accredited Red Team and an IATT or ATO, with more restrictive ROE for the testers. Non-certified adversarial testers and/or Red Teams may perform the CVI and ACD activities in a test enclave. When the system moves to the production network and connects with the interfacing systems, a certified Red Team is required.

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 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, if not corrected during the event. The CDT provides information to update the RMF POA&M and potentially the LCSP, with ACD test findings requiring corrective actions and uses ACD test results to inform updates to the PPP and Security Plan. Significant, mission-impacting vulnerabilities should be reported through the Program Office's formal DR process to ensure that cyber issues receive attention at the Program level for funding, if the contract language is inadequate or major engineering changes will be required. The CDT also provides ACD reports to the OTA and oversight organizations.



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

Evaluate Cybersecurity. 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. Not all exploitable vulnerabilities are mission impacting and the cybersecurity evaluation should properly categorize those vulnerabilities separately from mission impacting vulnerabilities to support the AO's ATO decision. The vulnerabilities that are not mission impacting should still be documented in the POAM in case the system's configuration changes resulting in mission risk from that vulnerability at a later time in the life cycle. 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 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, system cyber survivability, or operational 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 for OT&E.

Cybersecurity DT&E should answer the following questions at a minimum 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 mitigation and recovery capabilities perform as expected?
- What were the test limitations?

What are the results of the Operational Resilience Assessment?

- Did the system continue to operate during loss of information resources and connectivity?
- Did the system allocate information resources dynamically as needed to sustain mission operations while addressing cybersecurity failures?
- Did the system restore information resources rapidly to a trusted state within required mission thresholds?

What are the results of the System Cyber Survivability Assessment (if the system has a SS KPP)?¹⁴

- Did the system prevent engagements by cyber threat actors in order to prevent cyber intrusion, leaks and attacks? Evaluation includes, but is not limited to the following attributes:
 - Controlling access
 - Level of system’s cyber detectability
 - Securing transmissions and communications
 - Protecting system’s information from exploitation
 - Partitioning and ensuring critical functions are at mission completion performance levels
 - Minimizing, hardening and baselining attack surfaces
- Did the system mitigate cyber-attack effects to reduce mission impacts when attacks were successful? Evaluation includes, but is not limited to the following attributes:
 - Monitoring systems did/did not detect anomalies
 - Systems performance was manageable when system was degraded by cyber-attacks
- Did the system recover from cyber intrusions, leaks and attacks? Evaluation includes, but is not limited to the following attributes:
 - System recovery capabilities supported required timeframes for successful mission operations requirements (e.g., recovered software elements, configurations, and information from a trusted source)
- Does the system ensure that new threats are countered through hardware and software updates? How are patches managed and incorporated into system design, the LCSP, and in operations and maintenance in the operational environment to ensure that the system remains secure, survivable, and fully mission capable?
 - Updating security configuration baselines based on new threats
- What is the current CSRP?

What are the results of the Cybersecurity Standards 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?

¹⁴ *Cyber Survivability Endorsement Implementation Guide (CSE IG) v2.03*, Joint Staff/J6, Deputy DoD Chief Information Officer (CIO) for Cybersecurity, Defense Intelligence Agency (DIA), and the National Security Agency.



What are the results of the DCO assessments?

- How can the RMF continuous monitoring strategy be enhanced?
- Is the defense-in-depth strategy effective?
- Is the key cyber terrain identification included in the DCO analysis for triage prioritization?
- What does the digital environmental look like under normal conditions and when under attack?

What are the recommended corrective actions?

- For the PM?
- For the contractor?
- For the user?
- For the host environment, CSSP, and DCO?

7.4 Phase 4 Data Requirements

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

- ACD event assessment reports
- Informing 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
- An updated CSRP



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 2.7) 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 is to use data taken from cooperative cybersecurity test events to characterize the cybersecurity and operational resilience of a system in an operational context and provide reconnaissance of the system in support of the AA. 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.

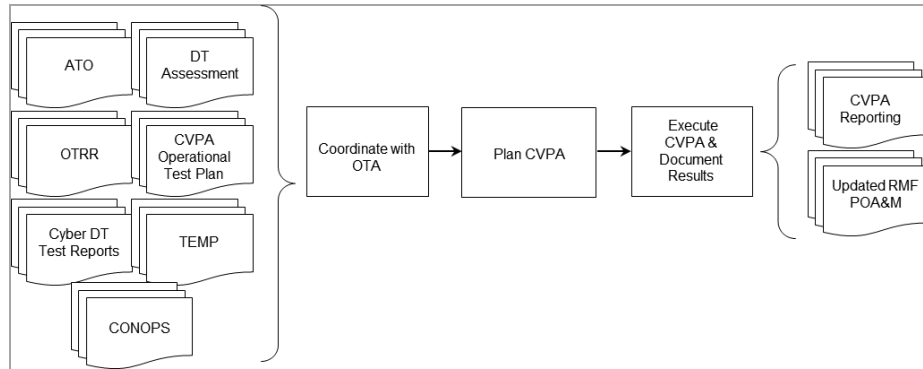


Figure 8-1. Phase 5: Cooperative Vulnerability and Penetration Assessment Activities

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. The OTA should attempt to schedule CVPAs far enough in advance of the AA to enable mitigation of vulnerabilities, but close enough to remain a relevant input to AA planning. Testing in this phase depends on the following considerations:

- **System developmental and design maturity.** The CVPA examines a production representative system 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 production representative systems for this evaluation when developing the test schedule. To the extent possible, CVPA events can be integrated with other test events, including developmental tests. For MDAPs, DOT&E will approve the selected approach as part of the test strategy in the TEMP.
- **Software/system maturity (status of previously identified deficiencies).** The CVPA begins either after previously identified CVI and ACD mission-impacting deficiencies have been resolved or with test plan documented mitigations. The test schedule must allow time to resolve the deficiencies 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 and other service-specific DOT&E activities conducted before

MS C require prior DOT&E approval. Not all programs require 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.

Service-specific A&A 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:

- Phase 1 and 2 artifacts
- System's PPP, SEP, and VOLT report
- System's CONOPS
- 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 mission-impacting deficiencies are resolved or mitigated and documented in the test plan and/or program's defect tracking system.
- 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.
- Service specific TRR 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.
- The draft CVPA Operational Test Plan for approval by the OTA (if created by the Service/component). The DOT&E April 2018 memorandum, appendix D describes details for the Operational Test Plan.



PMs should provide all necessary system documentation to the OTA and DOT&E, including but not limited to system architectures, network diagrams, SEPs, PPPs, 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, or if using specific teams to perform certain test activity functions, the OTA owns the assessment.

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 system attributes such as:

- Prevent: The ability to protect critical mission functions from cyber threats.
 - Relative to the NIST Cybersecurity Framework, Prevent includes both Identify and Protect activities.
- Mitigate: The ability to detect and respond to cyber-attacks and assess resilience to survive attacks and complete critical missions and tasks.
 - Relative to the NIST Cybersecurity Framework, Mitigate includes both Detect and React activities.
- Recover: The resilience to recover from cyber-attacks and prepare mission systems for the next fight.
 - Relative to the NIST Cybersecurity Framework, Recover includes the Recover activities.

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 assessments¹⁵:

- 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 CSE IG 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, as specified in 2018 DOT&E Memorandum, to conduct the CVPA.
- Authorized tools to assess system cybersecurity (typically the cybersecurity T&E team provides).
- Production-representative and operationally configured system; any test/system deviations must be identified to 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
- Representative system architecture, including supporting network infrastructure (routers, servers), and 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 enterprise or Service-level security services and service providers in support of the local network on which the SUT operates).”
- Results from a MBCRA, CTT, concept rehearsal, or similar analysis, available to DOT&E, the OTA, and teams supporting both the CVPA and AA

¹⁵ DOT&E Memorandum, *Cybersecurity Operational Test and Evaluation Priorities and Improvements* (27 Jul 2016)

- Operational test range(s) and system/network simulations where appropriate and authorized. The overall T&E schedule must include AA testing events.
- Cyber ranges, system integration laboratories, hardware-in-the-loop facilities, and laboratory environments if necessary, with appropriate verification, validation, and accreditation (VV&A) completed for OT&E. The Program Office must conduct verification and validation of the cyber range configuration, and the OTA must then accredit the cyber range configuration if plans include using a 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 Resources with the OTA

The OTA coordinates with the Program Office to identify the resources required for the Phase 5 events. Coordination should include establishing a schedule, desired capabilities, and expected products such as annexes to the operational test plan, data collection and reporting, and a formal report of activities and findings. If 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 captures and reports data and findings in accordance with the approved Operational Test Plan, the TEMP, and 2018 DOT&E Memorandum on minimum data and reporting. 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 that the authorized tools used to assess system cybersecurity are removed after testing is completed.

8.4 Outputs

The following are outputs from this phase, and should be completed before entering the next phase, Adversarial Assessment:

- The CVPA report documents all findings to include discovered vulnerabilities.
- The Program Office has developed a POA&M for all 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 (<https://www.dote.osd.mil/Publications/DOT-E-TEMP-Guidebook/>) provides guidance for cybersecurity content in the TEMP.

8.4.2 Acquisition Reviews and Decisions Informed by T&E

- MS C
- Low Rate Initial Production (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 effects to critical missions caused by threat-representative cyber activity against a unit training and equipped with a system as well as the effectiveness of the defensive capabilities.

This phase uses an NSA-certified Red Team accredited through the USCC to conduct testing for systems connected to the DoDIN. 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, equipment, threat assessment, safety and ongoing operations 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.

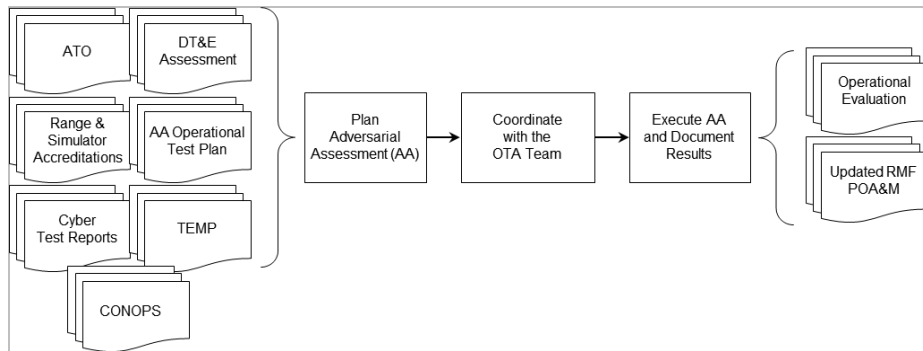


Figure 9-1. Phase 6: Adversarial Assessment Activities Schedule

9.1 Schedule

The OTA will conduct the events informing the AA. The AA can occur during or in support of the IOT&E. The duration of the AA will depend upon the details of the system design and cybersecurity threat 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 evaluate whether 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 mission-impacting cybersecurity deficiencies 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 approval of the TEMP and operational test plan (DOT&E for acquisition programs under oversight)
- Rules of Engagement for adversarial activities approved by all appropriate parties.
- Completed VV&A for all ranges, system integration laboratories, hardware-in-the-loop facilities, laboratory environments, and simulations involved in the event—the Program Office must conduct verification and validation and the OTA must accredit the test configuration if plans include using a cyber range, system integration laboratories, hardware-in-the-loop facilities, laboratory environments to support OT events.
- Completed training for the operators, system administrators, and network administrator 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. The OTA will complete planning in consultation with the CyWG and the Program Office. 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 to 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

Red and Blue Teams
While there are no set criteria for certifying Vulnerability Assessment Teams or Blue Teams, Red Teams performing operational testing on the DoDIN during formal OT&E must be certified by the NSA and accredited through USCC to ensure that 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.

- Representative system architecture, including supporting network infrastructure (routers, servers), and 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).
- 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 VV&A for the emulated system(s)

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

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

9.3.2 Coordinate with the OTA Team

The OTA coordinates with the Program Office to identify the resources required for the Phase 6 events. 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 TEMP.

9.3.3 Execute AA and Document Results

The OTA conducts the event and provides data and findings in accordance with the approved Operational Test Plan, the TEMP, and applicable guidance including the 2018 DOT&E Memorandum on minimum data and reporting. 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 that 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
- Program Office has developed a POA&M for remediating all major vulnerabilities

9.4.1 TEMP Updates

- The DOT&E TEMP Guidebook (<https://www.dote.osd.mil/Publications/DOT-E-TEMP-Guidebook/>) 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

10 Acronyms and Glossary of Terms

10.1 Acronyms

A&A	Assessment and Authorization
AA	Adversarial Assessment
ACD	Adversarial Cybersecurity DT&E
ACAT	Acquisition Category
AO	Authorizing Official
AOA	Analysis of Alternatives
API	Application Programming Interface
AT	Anti-Tamper
ATO	Authorization to Operate
ATP	Authority to Proceed
AVA	Architectural Vulnerability Assessment
BCAC	Business Capability Acquisition Cycle
BIOS	Basic Input Output System
CAN	Controller Area Network
CAPEC	Common Attack Pattern Enumeration and Classification
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDT	Chief Developmental Tester
CEVA	Cyber Economic Vulnerability Assessment
CIO	Chief Information Officer
CIP	Critical Intelligence Parameter
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COI	Critical Operational Issues
CONEMPS	Concept of Employment
CONOPS	Concept of Operations
COTS	Commercial off-the-Shelf
CPD	Capability Production Document
CPI	Critical Program Information
CSA	Cyber Survivability Attribute
CSO	Cloud Service Offering
CSP	Cloud Service Provider

CSRC	Cyber Survivability Risk Category
CSRP	Cyber Survivability Risk Posture
CSS	Contractor Service Support
CSSP	Cybersecurity Service Provider
CTM	Cyber Threat Modules
CTP	Critical Technical Parameter
CTT	Cyber Table Top
CVE	Common Vulnerabilities and Exposures
CVI	Cooperative Vulnerability Identification
CVPA	Cooperative Vulnerability and Penetration Assessment
CWE	Common Weakness Enumeration
CyWG	Cybersecurity Working Group
DAG	Defense Acquisition Guidebook
DASD	Deputy Assistant Secretary of Defense
DAST	Dynamic Application Security Test
DBS	Defense Business Systems
DCO	Defensive Cyber Operations
DEF	Developmental Evaluation Framework
DIA	Defense Intelligence Agency
DITL	Defense Intelligence Threat Library
DIV	Data and Information Viewpoint
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Networks
DOS	Denial of Service
DOT&E	Director, Operational Test and Evaluation
DR	Deficiency Report
DRFP-RD	Development Request for Proposal Release Decision
DSQ	Decision Support Questions
DT	Developmental Test
DT&E	Developmental Test and Evaluation
EMD	Engineering, Manufacturing, and Development
EW	Electronic Warfare
FDD	Full Deployment Decision

FRP	Full-Rate Production
GOTS	Government Off-the-Shelf
HWIL	Hardware-in-the-Loop
IAST	Interactive Application Security Test
IATT	Interim Authority to Test
ICD	Initial Capabilities Document
ICS	Industrial Control System
IOT&E	Initial Operational Test and Evaluation
IP	Internet Protocol
ISP	Information Support Plan
ISSM	Information System Security Manager
IT	Information Technology
ITT	Integrated Test Team
JCIDS	Joint Capabilities Integration and Development System
JFAC	Joint Federated Assurance Center
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Manual
KPP	Key Performance Parameter
KSA	Key System Attribute
KSAs	Knowledge, skills, abilities (see Appendix F)
LCSP	Life Cycle Sustainment Plan
LRIP	Low Rate Initial Production
MBCRA	Mission-Based Cyber Risk Assessment
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MEF	Mission Essential Functions
MS	Milestone
NCRC	National Cyber Range Complex
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OEF	Operational Evaluation Framework
OPFOR	Opposing Force
OPSEC	Operational Security
O&S	Operations and Support

Cybersecurity Test and Evaluation Guidebook 2.0, Change 1

OS	Operating System
OSD	Office of the Secretary of Defense
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTRR	Operational Test Readiness Review
OV	Operational View
OWASP	Open Web Application Security Project
PAT	Penetration and Adversarial Tester
PDR	Preliminary Design Review
PIT	Platform Information Technology
PM	Program Manager
PMR	Prevent, Mitigate, Recover
POA&M	Plan of Action and Milestones
PWS	Performance Work Statement
R&D	Research and Development
PPP	Program Protection Plan
RASCI	Responsible Accountable Supporting Consulted Informed
RF	Radio Frequency
RFP	Request for Proposal
RMF	Risk Management Framework
ROE	Rules of Engagement
SAST	Static Application Security Testing
SCA	Security Controls Assessor
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SE	Systems Engineering
SEP	System Engineering Plan
SIEM	Security Information and Event Management
SME	Subject Matter Experts
SOO	Statement of Objectives
SOP	Standard Operating Procedure
SoS	System of Systems
SRR	System Requirements Review
SS KPP	System Survivability Key Performance Parameter

SSE	Systems Security Engineer
STAT	Scientific Test and Analysis Techniques
STIG	Security Technical Implementation Guide
SUT	System Under Test
SV	Systems View
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
TPM	Technical Performance Measure
TRD	Technical Requirements Document
TRMC	Test Resource Management Center
TRR	Test Readiness Review
TSN	Trusted Systems and Networks
TTPs	Tactics, Techniques, and Procedures
USC	U.S. Code
USCC	US Cyber Command
USD(R&E)	Under Secretary of Defense for Research and Engineering
VA	Vulnerability Analyst
VOLT	Validated Online Lifecycle Threat
VM	Vulnerability Management
VV&A	Verification, Validation, and Accreditation
WIPT	Working Integrated Product Team

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 simulated 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 to define a group of individuals who 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 their findings and expertise, the Blue Team provides recommendations that integrate into an overall community security solution to increase the customer's cybersecurity 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 (CTPs)

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. CTPs should have a direct or significant indirect correlation to key CDD and, required system specifications or CONOPS. CTPs should be focused on critical design features or risk areas.

Cyber Table Top (CTT) 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, and 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 (Hypertext Transfer Protocol, File Transfer Protocol, Point-to-Point Protocol).

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 should 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 SEP 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 Cybersecurity SME is a person who demonstrates an authoritative knowledge in cybersecurity in respective areas. Different types of SMEs are needed who have background in cybersecurity for defense business systems, weapon systems, ICS, and HME systems.

Cybersecurity Survivability (Cyber Survivability)

The ability of a system to prevent, mitigate and recover to a known trusted baseline and maintain required mission operations.

Cyber Range

An event environment that supports cyber effects on information technology; weapons; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; 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.

Defensive Cyber Operations (DCO)

DCO provides the hardware, software, tools and staff to proactively protect and defend DoD networks and assets.

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 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, system cyber survivability, and operational 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 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

The Lead Systems Engineer is responsible for leading and implementing aspects of designing the system, to include 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. A CTT is an example of a methodology used to conduct an MBCRA.

Operational Resilience

The ability of a system to allocate information resources dynamically as needed to sustain mission operations while addressing cybersecurity failures, no matter the cause and restore information resources rapidly to a trusted state while maintaining support to ongoing missions.

Platform Information Technology (PIT)

PIT 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. PIT systems should be tested for cybersecurity effects. 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. Non-certified Red Teams may perform penetration and adversarial testing in a test enclave. When the system moves to the production network and connects with the interfacing systems, a qualified and certified Red Team is required. (Based on CJCSM 6510.03)

Red Team

A test team that emulates 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 (SCA)

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 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 (SSE)

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 (TTPs)

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 (T&E WIPT)

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 Chapter 8, T&E)

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, and 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 5000.02, Enclosure 14, Cybersecurity in the Defense Acquisition System, September 14, 2017
- DoD Instruction 8500.01, Cybersecurity, March 14, 2014, Incorporating Change 1, Effective October 7, 2019
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.03, Department of Defense Cyber Red Team Certification and Accreditation, February 28, 2013
- Defense Acquisition Guidebook, Chapter 8, “Test and Evaluation,” November 2, 2017
- DOT&E Memorandum, “Cyber Economic Vulnerability Assessments (CEVA),” January 21, 2015
- DOT&E Memorandum, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs,” April 3, 2018
- DOT&E Memorandum, “Cybersecurity Operational Test and Evaluation Priorities and Improvements”, 27 Jul 2016
- DOT&E Memorandum, “Operational and Live-Fire Test and Evaluation Planning Guidance for Middle Tier of Acquisition Programs”, October 24, 2019
- DOT&E Test and Evaluation Master Plan (TEMP) Guidebook, 19 January 2017, Version 3.1
- Joint Chiefs of Staff, Cyber Survivability Endorsement Implementation Guide v2.03
- NIST Special Publication 800-30, Rev 1, Guide for Conducting Risk Assessments, September 2012
- National Security Agency/CSS Technical Cyber Threat Framework v2 (NTCTF v2), 2 November 2018

References for Risk Management Framework (RMF):

- Committee on National Security Systems (CNSS) 1253, Security Categorization and Control Selection for National Security Systems, March 27, 2014
- DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014
- NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy, September 2017
- NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
- Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, “DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle,” Version 1, September 2015



Other References:

- Carnegie Mellon Software Engineering Institute, Special Report CMU/SEI-2018-SR-013. DoD Developer's Guidebook for Software Assurance, February 2018
- 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.
- DASD(SE) and DoD CIO, “Trusted Systems and Networks (TSN) Analysis”, June 2014
- Defense Acquisition University, “Incorporating Test and Evaluation into Department of Defense Acquisition Contracts”, October 2011
- DoD CIO, DoD Enterprise DevSecOps Reference Design Version 1.0, 12 August 2019

- DoD Chief Information Officer Memorandum, “DoD Cyber Hygiene Scorecard – Supplemental Guidance,” March 22, 2019
- DoD Instruction 4630.09, Enclosure 3, Communication Waveform Management and Standardization, October 10, 2017
- 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 5000.75, Business Systems Requirements and Acquisition, February 2, 2017
- DoD Instruction 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), November 17, 2017
- DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), November 5, 2012, Incorporating Change 3, October 15, 2018
- 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 8530.01, Cybersecurity and Cyberspace Defense Support to DoD Information Network Operations, Incorporating Change 1, July 25, 2017
- 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
- IEEE Computer Society, March 19, 1998, IEEE Guide for Information Technology—System Definition—Concept of Operations (ConOps) Document (IEEE Std 1362-1998)
- Institute for Defense Analysis, “State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation 2016”, Joint Requirements Oversight Council Memorandum (JROCM) 009-17, “System Survivability Key Performance Parameter Update to Ensure Joint Force Mission Assurance” January 26, 2017
- Joint Staff J-6, Warfighting Mission Area, Architecture Federation and Integration Project Portal, (U) Joint Common System Function List (JCSFL). <https://wmaafip.csd.disa.mil/Project?&aId=54>. (14 August 2018)
- MITRE ATT&CK™ Model. https://attack.mitre.org/wiki/Main_Page
- National Defense Authorization Act for Fiscal Year 2010, 10 U.S.C., Pub. L. 111-84 § 804, 2009
- National Security Agency/ Central Security Service Technical Cyber Threat Framework v2.
- Office of the Secretary of Defense, Director, Operational Test and Evaluation (DOT&E), Test and Evaluation Master Plan (TEMP) Guidebook, Version 3.1, January 19, 2017
- 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
- Office of the Chief Engineer (NAVWAR 5.0). Cybersecurity Technical Authority (CS TA), Cyber Risk Assessment (CRA) Standard Volume 1: Cyber Vulnerability Discovery Guide, 2019
- OUSD(R&E) Emerging Capability and Prototyping Office, DoD Prototyping Guidebook, December 6, 2018 (Version 1.0)
- USAF Systems Security Engineering (SSE) Acquisition Language Guidebook, Version 1.4, October 9, 2018.
- USC 392, “Executive Agents for Cyber Test and Training Ranges” December 2017
- US Department of Commerce, NIST Special Publication 800-160, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems November 2016
- 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 informed.

Table A-1. Cybersecurity T&E Acquisition and Review Decisions Quick Look

Cybersecurity T&E Functions	Decision and Review Points Influenced	Cybersecurity T&E Phase
Early Cybersecurity Tester Involvement Activities	<p>DoDI 5000.02: Milestone A, Developmental Prototype Review, SRR, Prototype and Milestone B Request for Proposals and Contract Awards, System Requirements Review (SRR)</p> <p>DoDI 5000.75: Solution Analysis Authority to Proceed (ATP), Functional Requirements ATP</p>	Phase 1
DT&E/OT&E Planning Activities	<p>DoDI 5000.02: SRR, Prototype down select, Preliminary Design Review (PDR), Capability Development Document (CDD) Validation Decision CDD-V, Development Request for Proposal Release Decision (DRFP-RD), Milestone B, Critical Design Review (CDR)</p> <p>DoDI 5000.75: Functional Requirements ATP, Acquisition ATP</p>	Phases 1, 2, 3
DT&E Test Execution Activities	<p>DoDI 5000.02: CDR, Milestone C, Low Rate Initial Production (LRIP)</p> <p>DoDI 5000.75: Limited Deployment ATP</p>	Phases 3, 4
OT&E Test Execution Activities	<p>DoDI 5000.02: Full Rate Production (FRP) or Full Deployment Decision (FDD)</p> <p>DoDI 5000.75: Full Deployment ATP</p>	Phases 5, 6

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.

Cybersecurity Test and Evaluation Guidebook 2.0, Change 1

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

	Phase 1 Understand Cybersecurity Requirements	Phase 2 Characterize Cyber Attack Surface	Phase 3 Cooperative Vulnerability Identification	Phase 4 Adversarial Cybersecurity DT&E
Inputs	<ul style="list-style-type: none"> • Capability Requirements Documents: JCIDS ICD, CDD, or Capability Production Document (CPD) • CONOPS • CSRC • DBS System Functional Requirements • PPP • SE Plan • DoDAF System Views or MBSE artifacts • DBS Design Specifications • DBS Capability Implementation Plan • VOLT report, CTMs from the DITL • RMF Security Plan • RMF Security Assessment Plan • MBCRA, if available • Previous cybersecurity vulnerability assessment reports, penetration testing reports or AA reports, if available • CSSP Support Agreement 	<ul style="list-style-type: none"> • Cybersecurity requirements and requirements traceability documentation • CSRC • CONOPS, CONEMP, User manuals • DBS Capability Implementation Plan • DBS Capability Support Plan (if available) • CSSP Support Plan • Information Support Plan (ISP) • DoDAF OVs, SVs, DIVs or MBSE artifacts • DBS Design Specifications • System Design Documents • System Interface Control Document • Lists of system hardware and software • List of critical components including detail for all logic-bearing devices to the component level and information necessary to conduct threat assessments of critical item suppliers • RMF Security Plan and Security Assessment Plan • Authorization boundary diagrams including systems and data flows • PPP • System Threat Assessment • SEP • TEMP and DEF • MBCRA 	<ul style="list-style-type: none"> • Cybersecurity portion of the DEF • Attack Surface Analysis Report from Phase 2 • Test results from contractor T&E activities (prototypes, sub-components, integration testing) • Test results from contractor component-level testing, and contractor integration testing • Test results from contractor full system testing • Verification of fixes reports • Software Requirement Specification • Software Test Plan and software assurance test results • DBS Capability Implementation Plan • DBS Capability Support Plan • Test Strategy for Phase 3 • Updated TEMP • RMF Security Assessment Plan • RMF Security Plan • CONOPS, CONEMP, User Documentation • MBCRA results 	<ul style="list-style-type: none"> • Cybersecurity requirements and requirements traceability documentation • 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 • CSRP • Mature and stable system baseline • CONOPS, CONEMP, User documentation • MBCRA
Major Tasks	<ul style="list-style-type: none"> • Compile list of cybersecurity standards, system cyber survivability and operational resilience requirements <ul style="list-style-type: none"> • Examine cybersecurity standards • Examine operational resilience requirements • Examine system cyber survivability requirements • Prepare for cybersecurity T&E events <ul style="list-style-type: none"> • Develop the initial DEF • Identify supporting cybersecurity T&E resources • Develop the initial OT evaluation framework • Align RMF activities with the TEMP • Align DCO capabilities to support RMF • Plan and schedule an MBCRA • Plan for cybersecurity T&E <ul style="list-style-type: none"> • Develop cybersecurity T&E strategy 	<ul style="list-style-type: none"> • Identify the cyber-attack surface <ul style="list-style-type: none"> • Examine system architecture, components, and data flows • Analyze and decompose system mission • Map mission dependencies • Analyze the attack surface <ul style="list-style-type: none"> • Characterize the cyber threat • Select a cyber kill chain • Examine cyber effects on the system and mission • Perform or update MBCRA • Document results and update test planning and artifacts <ul style="list-style-type: none"> • Document results of cyber-attack surface analysis in a cyber-attack surface analysis report • Develop threat vignettes (use cases) to guide test planning • Prepare for Phase 3 CVI and Phase 4 ACD events <ul style="list-style-type: none"> • Formulate test strategy • Schedule 	<ul style="list-style-type: none"> • Plan CVI Test Activities <ul style="list-style-type: none"> • Develop cybersecurity test objectives • Test security standards • Test operational resilience • Test system cyber survivability • Plan and schedule test events • Test plan documentation • Plan cyber test infrastructure • Integrated system testing • Conduct CVI events and document results <ul style="list-style-type: none"> • Obtain reports • Cybersecurity evaluation • Update MBCRA • Prepare for Phase 4 ACD events 	<ul style="list-style-type: none"> • Update cyber threat assessment and attack surface analysis • Plan adversarial DT&E <ul style="list-style-type: none"> • Schedule, Develop test objectives, • Test operational resilience, Test system cyber survivability, Test4 security standards • Integrating Government Phase 4 and Phase 5 • Define metrics, identify resources, develop ROE • Define process and test cases • Plan integrated tests • Document test plans • Finalize preparation of test infrastructure • Conduct TRR for ACD • Conduct adversarial cybersecurity DT&E <ul style="list-style-type: none"> • Perform ACD events • Obtain reports • Cybersecurity evaluation • Exit criteria for cybersecurity DT&E

Cybersecurity Test and Evaluation Guidebook 2.0, Change 1

	Phase 1 Understand Cybersecurity Requirements	Phase 2 Characterize Cyber Attack Surface	Phase 3 Cooperative Vulnerability Identification	Phase 4 Adversarial Cybersecurity DT&E
Outputs	<ul style="list-style-type: none"> • Cybersecurity standards, system cyber survivability and operational resilience requirements and other factors that influence cybersecurity testing • Inclusion of T&E items within the prototype and system development RFPs • Updates to MBCRA 	<ul style="list-style-type: none"> • Attack surface analysis report • List of interfacing systems and data connections that may expose the system to potential threats • Identified attack-surface protection responsibilities • List of known vulnerabilities in the system • Cybersecurity T&E resource requirements • Updates to MBCRA • Updated TEMP 	<ul style="list-style-type: none"> • Details of test conduct • Description of the SUT and relevant interfaces for testing • Formal CVI reports • Cybersecurity evaluation to include assessing the CSRP • Evidence that known system vulnerabilities are either remediated or enumerated and tracked • Plan for at least one ACD event • Verification of T&E infrastructure requirements for Phase 4 • Updated MBCRA of system vulnerabilities based on Phase 3 T&E results to inform Phase 4 planning and acquisition decision events • TEMP Updates 	<ul style="list-style-type: none"> • ACD event assessment reports • Updated RMF POA&M • Cybersecurity evaluation • Updates to MBCRA • Updated CSRP • TEMP updates

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

	Phase 5 Cooperative Vulnerability and Penetration Assessment	Phase 6 Adversarial Assessment
Inputs	<ul style="list-style-type: none"> • Phase 1 and 2 artifacts • Authorization to Operate • Test results from contactor DT&E • Identification of mission-impacting deficiencies • Resolutions to identified mission impacting deficiencies • Completion of residual DT&E • Updated cybersecurity evaluation • Operational Test Readiness Review • Approval of operational test plan by appropriate authority • Updated MBCRA 	<ul style="list-style-type: none"> • Authorization to Operate • Test results suggestive that system is capable of operation in intended environment • Remediation (verified fix, or documentation) of all mission-impacting deficiencies previously identified • Approval of operational test plan by appropriate authority • Verification, validation, and accreditation for all ranges and simulations to be involved in the event • Training completion for operators, system administrators, and network administrator • Recent MBCRA results
Major Tasks	<ul style="list-style-type: none"> • Plan CVPA • Coordinate with OTA • Execute CVPA • Document results 	<ul style="list-style-type: none"> • Plan adversarial assessment • Coordinate with the OTA team • Execute the adversarial assessment • Document results
Outputs	<ul style="list-style-type: none"> • DOT&E Memorandum identifies the minimum expected data • CVPA report with discovered vulnerabilities • POA&M for remediating all major vulnerabilities • Documented operational implications of non-correctable vulnerabilities • Updated MBCRA 	<ul style="list-style-type: none"> • DOT&E Memorandum identifies the minimum expected data • Operational evaluation • Updated MBCRA

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 Guide*¹⁶. 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 PM may tailor the T&E guidance to fit their unique program situation or acquisition strategy. 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 or equivalent tailored document and updated at each milestone/decision point 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 as 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 cybersecurity testers need to understand the contractor testing processes to include cybersecurity testing, 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. A best practice is to pursue integrated government and contractor testing during development to share intelligence with the contractor, test tools and techniques the government will use in order to optimize the find-fix-retest opportunities before the system engineering is no longer adaptable.

¹⁶ 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

An 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 sample work statement language (Section C) as well as information that can be required and evaluated from the offeror.

B.2.1 Section C – General Cybersecurity T&E Contract Requirement Considerations

Section C of the RFP contains the detailed description of the products to be delivered or the work to be performed by the contractor under the contract. This section includes the government's contract requirements typically documented in a SOO, SOW, or Performance Work Statement (PWS) and preliminary System Performance Specification.

The following are examples that can be used as a starting point and modified for unique considerations of each program's SOW. Programs should also review Appendix X5 to identify contract language applicable for non-IP systems.

Support Government-Led Activities

- 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 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)



System Documentation and Design Reviews to Support Government Test Planning

- 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
- Conduct a criticality analysis to accurately identify and compile a parts list for all critical components
- Produce a critical component list that includes the break down for all logic-bearing devices to the component level and all key information necessary to conduct threat assessments of critical item suppliers
- Provide detailed design and architecture documentation to support test planning activities.
- Work with government testers to identify potential security weaknesses, functional deficiencies, and or vulnerabilities in support of formal and informal design reviews
- Identify cyber dependencies that may impact dependent systems that are internal and external to the SUT (e.g. sub-contractor supplier components, external software libraries, proprietary software libraries, avionics, backup power, HVAC, commercial cloud, etc.)

Contractor Testing

- Collaborate with government testers to develop test cases and test scripts
- 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 T&E on components and sub-components as described in the TEMP
- Conduct Phase 3 and 4 testing and repeat the two phases as needed to eliminate discovered vulnerabilities until delivery to the government for government CVI and ACD events
- Conduct ACD with integrated government testers before delivering the system to the government for government DT&E. Allow enough time to mitigate vulnerabilities found during the ACD before Phase 5
- 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
- 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.
- 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
- Verify DISA Security Technical Implementation Guides (STIGs) compliance posture
- Identify and test protocols not covered by STIGs as specified by program SE
- 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.
- Test for vulnerabilities that may impact dependent systems that are internal and external to the SUT (e.g. sub-contractor supplier components, external software libraries, proprietary software libraries, avionics, backup power, HVAC, commercial cloud, etc.)
- Provide government access to data from contractor cybersecurity test events
- Provide government access to contractor development environment and facilities for Defense Contractor Management Agency (DCMA) to assess cybersecurity supply chain risk



Integrated Contractor-Government Testing

- Work with government test engineer(s) to document methodologies for integrated contractor-government testing that meets the needs of the program while adhering to acquisition timelines
- Participate in integrated contractor-government vulnerability assessment teams to conduct CVI and ACD test events
- Collaborate with integrated government testers to facilitate sharing sanitized or relevant cyber threat intelligence information to support contractor ACD events

Contractor Reporting and Deliverables (Example Data Item Descriptions)

- Develop and deliver contractor detailed test plans for contractor test events (DI-MGMT-82140)
- 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 (DI-MGMT-82141)
- Analyze and evaluate test results in a T&E Report for each test event. (DI-MGMT-82142)
 - Track contractor-identified vulnerabilities and corrective action/mitigation plans (GFE/GFI: DI-MGMT-82146, RMF DI-MGMT-82135, Vulnerability Scan DI-MGMT-81842)

- Provide reports of residual vulnerabilities to government vulnerability assessment and ACD test teams (RMF DI-MGMT-82135)
- Identify any cybersecurity-related data products contractors must provide. Define CDRLs and select applicable DIDs.

Government Product Acceptance Testing

- Provide a digital twin of the system, System Integration Lab or Hardware in-the-Loop facility for government 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, system cyber survivability, and operational resilience developmental testing.
- Fix and verify vulnerabilities identified as exploitable and mission impacting cyber deficiencies during government product acceptance testing. Vulnerabilities discovered during government product acceptance testing will result in non-acceptance and product return to the contractor for remediation.

B.2.1.1 Cybersecurity T&E Contract Considerations for Cloud Deployments

For more information on contract language for cloud deployments, refer to the *Cloud Cybersecurity T&E Addendum* at <https://www.dau.edu/cop/test/Pages/Documents.aspx>

B.2.1.2 Cybersecurity T&E Contract Considerations for DevSecOps:

- Collaborate with government development, testing, security and operations teams early and often to encourage automation to enable consistent and repeatable testing, security, integration, delivery and deployment practices throughout the delivery pipeline
- Programs should ensure that government testers can audit the contractor development facilities to ensure that automated security testing is in fact occurring during the software development process.
- Programs should also ensure that the development environment is secure and free from compromise by adversaries while software development is occurring.
- Programs should request via development contracts and then verify that the development environment is staffed by known, vetted, trusted personnel, and uses secure, malware-free tools, libraries and scripts.

For more information about contract language for DevSecOps testing consult Appendix C and refer to the following reference: DoD CIO, *DoD Enterprise DevSecOps Reference Design Version 1.0*, 12 August 2019

B.2.1.3 Cybersecurity T&E Contract Considerations for Testing of Prototypes

- Include prototype end-user and testing professionals in developing the T&E scope, objectives, approach, and schedule
- Work with the government early in the planning process to ensure that the type of test and evaluation and the test environment will provide the data and information needed to satisfy the prototyping project's purpose
- Expect and allow government use of independent assessors to help plan and conduct prototype evaluations and/or analyze the data generated
- Collaborate with the government to assess product quality and cybersecurity risk factors for prototypes that are intended for transition to operational use

For more information about contract language for testing of prototypes, refer to the following reference: DoD Prototyping Guidebook, published by the OUSD(R&E) Emerging Capability and Prototyping, December 6, 2018 (Version 1.0)

B.2.1.4 Cybersecurity T&E Contract Considerations for Software Testing

Software Development

- Secure the development environment and test the development environment to ensure it can detect cyber-attacks.
- Allow government personnel access to prime and subcontractor development environments to assess and inspect the security of the development and test environment.
- Ensure any contractor development environment is physically and logically isolated from other networks, to include its enterprise unclassified network in accordance with NIST SP 800-171.
- Develop and test the system to demonstrate that the system deters (prevents), detects (responds), and recovers from cyber-attack
- Develop, test, and deliver a system that is resilient in a cyber-contested environment
- Develop a secure coding guide that specifies language, required constructs/practices/patterns, prohibited constructs/practices/patterns, software comment requirements for use by coders
- Implement formal (e.g., Fagan) design and code inspections
- Verify all code against the CWE, CVE, and OWASP vulnerability data bases
- Perform an origin analysis of all third-party libraries and frameworks used and ensure the versions used in the delivered software have no publicly known vulnerabilities and continue to review for newly reported vulnerabilities throughout the sustainment of the delivered software
- 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
- Ensure all developers are trained and held accountable for secure code development

Software Interfaces

- Completely document all software interfaces from the contractor developed system
- Completely document testing performed for data validation, strong typing, and range checking

Software Tools

- Utilize automated tools to support software configuration control
- Utilize automated testing tools to support regression testing for all custom code with at least 90% statement coverage
- Utilize at least two different commercial static analysis tools to measure software quality and access vulnerabilities. Multiple tools are to be used to improve detection of software quality issues and vulnerabilities as each tool uses different detection methods

Applicability and Scope of Software Assurance

- Software assurance requirements apply to all software delivered by the prime contractor. Should the prime contractor employ subcontractors, then the prime contractor shall require software assurance requirements from each subcontractor they employ for use on the contract
- All software assurance requirements defined in the contract shall apply to all reused code included and delivered by the prime contractor and its subcontractors
- All software assurance requirements defined in the contract shall apply to all reused objects, both proprietary and open source, and their originating reused source code, whether that code was

included and delivered by the prime contractor and its subcontractors or just referred to by them as the source of the reused object

Software Assurance Reporting

- Provide reports to support government T&E that:
 - Describe how static analysis for software assurance is used within the development life cycle in writing and in diagram form for illustrative purposes
 - Describe the output from a minimum of two software static analysis tools used
 - Describe static analysis test results of the legacy code provided
 - Provide a prioritization of severity for defects and vulnerabilities

Vulnerability Management

- Conduct quarterly software vulnerability assessments along with a monthly patch management cycle and follow local procedures for out-of-band patches
- Coordinate with government personnel creation and implementation of processes that identify and correct or mitigate vulnerabilities and defects and ensure documentation is included in the LCSP

For more information about software testing practices, refer to Appendix G

B.2.2 Section L – Instructions to Offerors or Respondents

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.

Examples for Section L:

- The offeror shall describe their overall plan and methodology for how the cybersecurity, system cyber survivability and operational resilience requirements will be managed, tested, evaluated and flowed down to subsystems and components including those that subcontractors/development partners have provided including 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 provide an approach for integrated contractor and government test that will be used throughout development and integration of the required system capability
- The offeror shall describe their approach to cybersecurity risk management, including threat analysis, system exposure to threats, and integration of cybersecurity with systems engineering and risk management processes
- The offeror shall describe how their process align with the activities described in the DoD Cybersecurity T&E Guidebook
- The offeror shall describe their process to ensure that 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
- The offeror shall describe their approach to implementing a defense-in-depth-strategy in support of assessing DCO
- The offeror shall describe their process for fixing and verifying exploitable and mission impacting cyber deficiencies that have been identified by government testing and describe how they will confirm that no new known vulnerabilities have been introduced during remediation
- The offeror shall describe their processes for monitoring cybersecurity supply chain risk that may be mission impacting
- The offeror shall describe their overall plan and processes for software assurance development and testing, including:
 - Secure coding processes and practices that include minimizing unsafe function use, using static and dynamic analysis tools, performing manual code reviews, and leveraging CWE, CVE, OWASP tools and guidance, and CAPEC analysis. Describe and address the following concepts, practices, and procedures: design inspection, code inspection, penetration testing, planned annual test coverage, failover multiple supplier redundancy, fault isolation, least privilege, system element isolation, input checking/validation, software load key, development environment source code availability, development environment tool release testing, generated code inspection, access controls in the development environment, cybersecurity controls in the development environment, and controlling/accounting for technical manuals¹⁷
 - Approach for testing security-related operational resilience to include protection/deterrence, detection/monitoring, constraining/isolating, maintaining/recovering, and adapting¹⁸
 - Process for identifying cybersecurity key risks, vulnerabilities, and threats to important assets and functions provided by software applications¹⁹

B.2.3 Section M – Evaluation Criteria

Section M, “Evaluation Factors for Award,” or Evaluation Criteria 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.

Examples for Section M:

The Government will evaluate the proposed approach to cybersecurity, system cyber survivability, and operational resilience and assess the degree to which it will identify the system’s threat exposure. The evaluation will further focus on:

- The contractor’s process to fix and verify exploitable and mission impacting cyber deficiencies identified by government testing and how they will confirm that no new known vulnerabilities have been introduced during remediation

¹⁷Language adapted from: USAF Systems Security Engineering (SSE) Acquisition Guidebook, 8 May 2018, Version 1.3.

¹⁸ Ibid

¹⁹ Ibid

- The contractor's process to monitor their development environment for cybersecurity supply chain risks that may be mission impacting
- The completeness with which the offeror addresses vulnerability assessment, malicious code insertion, and threat assessment²⁰
- The contractor's process for finding and fixing exploitable and mission impacting cyber deficiencies, mitigating threats, vulnerabilities, and risks, including how resiliency architecture will be tested including²¹
 - Tracking all vulnerabilities uncovered during the entire contract lifecycle
 - Controlling the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources
 - Detecting the occurrence, reducing the likelihood of occurrence, and mitigating the consequences of products containing counterfeit components or malicious functions
 - Cybersecurity risk reduction strategies (e.g., domestic sourcing from trusted foundries)

The Government will evaluate the proposed approach to software assurance testing as it relates to secure software development practices to be used during the software design, development, integration, and test phases of the program, to including minimizing unsafe function use, using static and dynamic analysis tools, and performing manual code reviews. The evaluation will further focus on:

- Testing methodologies to be used, including code evaluations, functional testing, penetration testing, fuzz testing, vulnerability scans, third-party assessment, and off-nominal testing²²
- Security processes to develop, maintain, and manage software securely (including unclassified and classified software)²³
- Implementing CWE, CVE, OWASP tools and guidance, and CAPEC analysis²⁴
- Managing cybersecurity patches, updates, and implementation of configuration control, including descriptions of both engineering and formal code control²⁵

The Government will evaluate the extent to which the offeror's proposed integrated contractor and government test approach maximizes test and evaluation efficiencies and minimizes redundancy.

²⁰ Ibid

²¹ Ibid

²² Ibid

²³ Ibid

²⁴ Ibid

²⁵ Ibid

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 traditional DoDI 5000.02 full acquisition life cycle. This ideal case allows enough time for planning cybersecurity test activities with contractor and government engineers and cybersecurity test teams. However, the Office of the Secretary of Defense (OSD) advocates multiple adaptive acquisition models to promote rapid fielding, rapid prototyping, DevSecOps, Agile, and other approaches to deliver capability more quickly to the warfighter. Figure C-1 illustrates the Adaptive Acquisition Framework Pathways. 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.

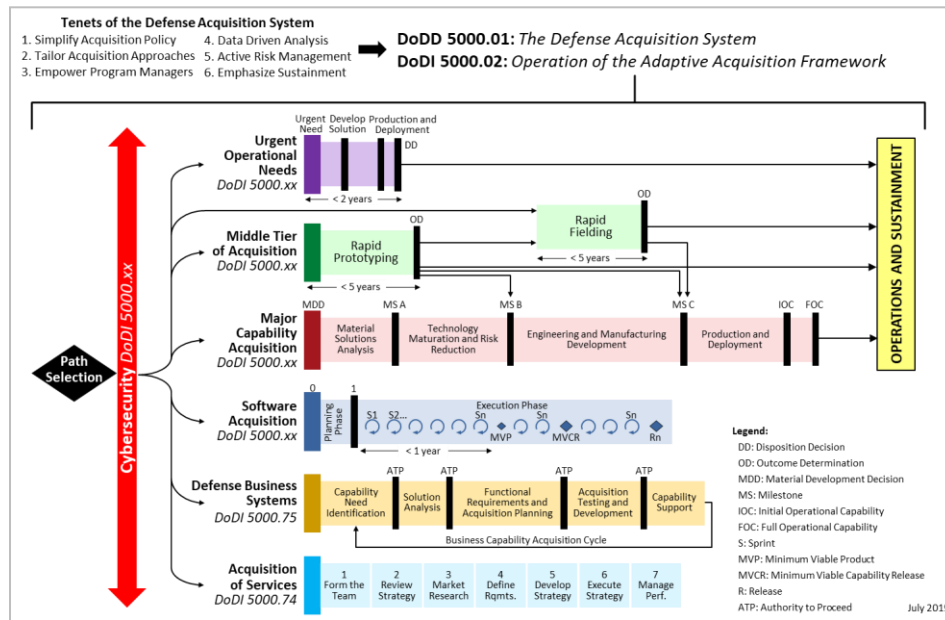


Figure C-1. Adaptive Acquisition Framework (AAF) Pathways

This Appendix advocates tailoring and integrating, not skipping, the phases. When tailoring the phases, CDTs continue to follow the general principle that *cybersecurity testing should occur as early as possible and during system development*. Early execution of Phases 1 and 2 and iterating them during the testing supports a continuum of analysis to address both the evolving threat and system design and requirements. Early and regular discovery of mission impacting 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.

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 the timing and scope of cybersecurity T&E. CDTs and OTAs should understand and document the cybersecurity risks associated with what testing can and cannot be accomplished in each tailoring scenario. The CDT should tailor the phases to the desired timeframe, not tailor out or skip phases. CDTs and OTAs document the tailored test strategy 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. Figure C-2 represents the Cybersecurity T&E six-phase process independent of any acquisition model. This process promotes integrated contractor and government testing during the early development efforts (prototypes included). The figure advocates an iterative effort with Phases 1 and 2 analyses informing the test-fix-re-test efforts in each phase. The tailored Cybersecurity T&E six Phase process also promotes continuous testing for agile development and DevSecOps programs. Programs should tailor the testing performed during phases to match the timeframe when the capability is needed by the end-user.

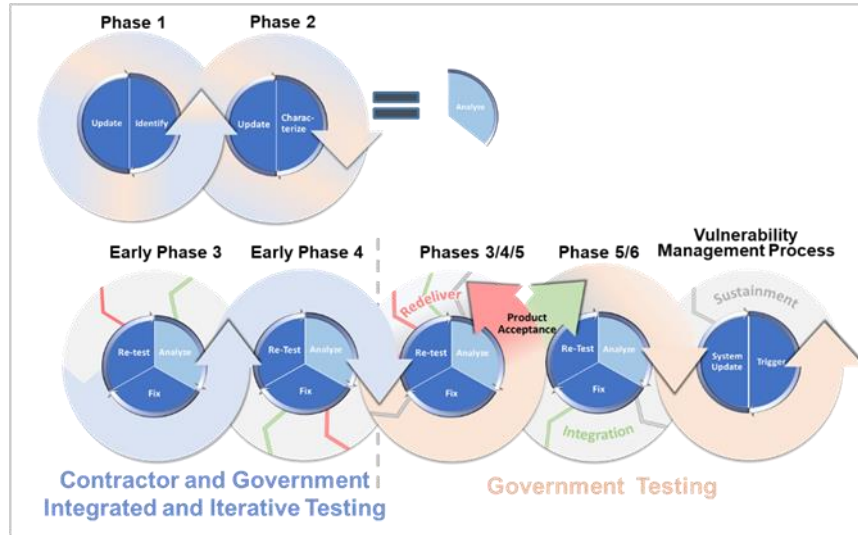


Figure C-2. Tailored Cybersecurity T&E 6 Phase Process

Analysis: Phases 1 and 2 – The purpose of the analysis phase is to understand the capability needed, the desired timeline for delivery, cybersecurity requirements, and cyber threats to the system and how they may impact the mission. Phases 1 and 2 activities plan the people, tools, and infrastructure needed for subsequent test phases and directly inform the T&E language to put into prototype and development RFPs and contracts. The analysis wedge is iterative; it is performed and updated in each test phase and is required for both contractor and government test activities. MBCRAs are conducted during Phases 1 and 2 analysis to focus test priorities.

Contractor and Government Integrated Testing: Early Phases 3 and 4 – During early Phases 3 and 4, contractors conduct cybersecurity testing during system development with government oversight or assistance. When a prototype or a system is not be available for testing, contractor developmental testing addresses all hardware and software components and sub-components, sub-system testing and integrated system testing. The scope of contractor testing also includes the security of the development environment: development processes, code libraries, test tools, and personnel vetting. Integrated contractor and government teams conduct vulnerability assessments and penetration testing to examine adequacy of the cybersecurity controls, and adversarial testing to assess operational resilience and system cyber survivability requirements.

Suggested contract language considerations include Phases 3 and 4 activities and test objectives (refer to Phases 3 and 4 in this Guidebook), test automation during system development, periodic auditing of the contractor development environment, greater visibility into software testing, and government oversight and involvement to ensure iterative and integrated test. For information about suggested contractor cybersecurity T&E contract language to support contractor early Phases 3 and 4, refer to Appendix B.

Integrated DT/OT: Phase 3/4/5 - Phase 3/4/5 is integrated government DT/OT that occurs with each release of the hardware and software capability from the contractor. The purpose is to verify contractor testing and conduct government cybersecurity acceptance testing. Government testing finds and fixes vulnerabilities, and retests systems to verify fixes. To prepare for Phase 3/4/5, the CyWG reviews contractor test results and conducts an MBCRA to guide additional testing. Acceptance testing may include the following activities:

- Auditing of the contractor development environment, tools, and processes
- Cybersecurity standards testing
- Operational resilience testing (system and data recovery testing)
- System cyber survivability testing
- Supportability and maintainability testing - DCO monitoring, logging and auditing, threat detection
- Interfacing system exposures that impact missions

To support Phase 3/4/5, the contract requires language to address the criteria for government rejection of the product based on cybersecurity defects with mission impact. Contract language should require contractors to prioritize fixing mission impacting vulnerabilities. Products may be rejected as not resilient, not survivable, and/or not meeting security standards.

OT Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA): Phase 5/6 – Government OTAs conduct the CVPA and AA. The OTAs consider applicable results from previous integrated testing and Phases 1 and 2 analysis when planning the CVPA and AA. The testing is performed in a representative operational environment. The AA is performed from the standpoint of operators using a system to execute missions and tasks in the expected operational environment that includes adversarial cyber activity.

Vulnerability Management Process – The Vulnerability Management (VM) process during operations and sustainment ensures that systems remain in an acceptable risk posture. FOT&E may include VM test activities and test data from the following assessments: the Information Assurance Vulnerability Alerts (IAVA) process, RMF A&A and continuous monitoring processes, formal configuration management, periodic vulnerability and penetration testing, Combatant command exercises, Deep Cyber Resilience Assessment and other assessments, CSA 10 requirements, other system sustainment requirements and DCO protections. When needed engineering or functional changes trigger a return to acquisition (new RFP, new contract, DT&E and OT&E), the CyWG needs to perform Phases 1 and 2 activities, to include an MBCRA, to account for the system’s current security posture. Assessing the current cyber posture before moving forward will help avoid carrying old vulnerabilities and bad habits (people, processes, technology) into a new system by exposing security deficiencies that can be remediated in the next version of the system. For example, if the system is being used incorrectly or insecurely, then any security deficiencies discovered during operations could be corrected in the next release.



The sections below provide tailoring considerations for rapid prototyping and rapid fielding programs, 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.

C.1 Tailoring for Rapid Prototyping and Rapid Fielding Programs

Accelerated acquisition programs bring modified or new capabilities to the field within 6 months and complete fielding in five years. Rapid prototyping and fielding programs require tailored cybersecurity T&E processes that keep pace with rapid acquisition and fielding timelines. Rapid acquisition programs are likely dependent on contractor test programs to help release capabilities to the field more rapidly. The

accelerated timeline is dependent on good contractor testing during system development. While government independent testing will be performed, it may reveal problems too late. Late discoveries often lead to delays to the production timeline or release of systems to the field that are vulnerable to cyber-attacks. Contractor cybersecurity testing must “shift left” to include better and continuous software testing during development, testing for security standards (RMF controls), operational resilience, and system cyber survivability requirements to enable faster deliveries that do not sacrifice security features.



Often, accelerated acquisition programs are software-intensive and feature frequent software releases and automated testing. Automated testing that occurs continuously during development and deployment enables faster delivery of capabilities to the field. To facilitate frequent software releases, test engineers are embedded in the software development process. Another characteristic of accelerated acquisition programs are their heavy dependence on COTS or non-developmental items (NDIs) technology which expands the system’s attack surface and supply chain risk from an adversary viewpoint. If the system uses an Agile software development model and/or DevSecOps development processes, see Section C.2 for additional tailoring information.

Software intensive systems should ensure that the contract has well defined software assurance and security testing requirements for each delivery build, and language supporting government tester integration into the development process. The development environment, development processes, secure coding practices and development tools should be scrutinized. 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.

C.1.1 Rapid Prototyping

Rapid prototypes can be demonstrated in an operational environment and provide residual operational capability within five years of an approved requirement. The goal of cybersecurity T&E for early prototyping activities is to examine prototype designs for inherent vulnerabilities in architecture, hardware, and software that cannot be easily secured or remedied. Also, cybersecurity T&E should examine interface risks and system maintainability to ensure that the prototype can be easily updated to maintain the required security posture if it is fielded. Programs should conduct MBCRAs to uncover and analyze cyber vulnerabilities that may have adverse mission impacts so they can be fixed as early as possible in the development life cycle. MBCRAs inform prototype design, development, test and fielding activities. Cybersecurity testing during OT&E assesses the ability of the system to enable operators to execute critical missions and task in the expected operational environment.

Cybersecurity test considerations for rapid prototyping include:

- Use of innovative technologies that may not have been completely assessed for cybersecurity
- Rapid development requires focusing on critical issues; not all cyber vulnerabilities will be mitigated; residual cyber vulnerabilities should be documented.
- Tailoring integrated test events expedites the development schedule
- Early tester involvement, such as embedding testers with developers, facilitates early vulnerability detection

Analysis: Phases 1 and 2 – Testers help programs assess risks to critical systems and missions that will use the prototype. Access to prototypes during early design and development activities can help government test planners better target security testing and adhere to rapid program timeframes.

Integrated Contractor-Government Testing: Phases 3 and 4 - CDTs should plan to embed government test engineers into the contractor prototype design and development activities to provide oversight for continuous cybersecurity T&E. Using test automation during system development, code is examined for anomalies that could create system vulnerabilities.

Integrated DT/OT: Phase 3/4/5 – Formal acceptance testing occurs during each release of the prototype hardware or software capability. The CyWG evaluates data from contractor testing or RMF assessments to plan remaining testing. CDTs conduct periodic auditing of the contractor development environment and processes for security flaws.

OT CVPA and AA: Phase 5/6 - Adversarial testing is conducted in an operationally relevant demonstration near the end of the initial prototype development period and before initiation of the rapid fielding effort if the prototype will be fielded. The OTA will consider applicable information from completed testing when identifying and planning the events needed for the CVPA. If enough data from previous test events is not available to support adversarial testing, then dedicated activity will be needed to guide AA test planning.



C.1.2 Rapid Fielding Programs

Rapid fielding programs promote the use of proven technologies to field production quantities of new or upgraded systems with minimal development required. The objective of a rapid fielding program is to begin production within six months and complete fielding within five years of the requirement.²⁶ A rapid program can proceed from approved requirement directly to production with minimal development or as a follow-on to a rapid prototype.

The nature of rapid fielding programs makes the government highly dependent on the quality of cybersecurity testing performed by the development contractor. This increased dependence on contractor testing extends to the security of the contractor’s development environment and development processes. 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 providing contractor design documentation and cybersecurity T&E data to the government, and government observation of contractor cybersecurity T&E.

The selected proven technology may not have previously undergone cybersecurity testing to expose systemic vulnerabilities and analyze supply chain issues. Minimal development time does not mean minimal testing. The CDTs and T&E Leads should examine previous test results and plan to test any items that were not covered in the previous testing. If the technology is using Agile software development techniques and DevSecOps processes, refer to section C.2 for more information.

Cybersecurity test considerations for rapid fielding programs include:

- Proven technologies may not have had adequate testing for cyber vulnerabilities before fielding
- Proven technologies are often already known to cyber adversaries
- Inherited technologies often contain inherited vulnerabilities
- Rapid development requires focusing on critical issues; not all cyber vulnerabilities will be mitigated; residual cyber vulnerabilities should be documented
- Tailoring integrated test events expedites the development schedule
- Early tester involvement, such as embedding testers with developers, facilitates early vulnerability detection

²⁶ USD(R&E). *Middle Tier of Acquisition (Rapid Prototyping/Rapid Fielding) Interim Governance*, October 9, 2018

Analysis: Phases 1 and 2 - Government testers should review design documentation for the proven technology and review any previous test results. The Program VOLT Report, design documentation and previous test results can help testers better target any additional security testing needed.

Integrated Contractor-Government Testing: Phases 3 and 4 - Vulnerability assessments and penetration testing should be conducted if not performed previously or if test results are not available.

Integrated DT/OT Phase 3/4/5: See Rapid Prototyping Section C.1.1

OT CVPA and AA: Phase 5/6 – Conduct integrated developmental and operational testing to demonstrate how the proven technology contributes to fulfilling the warfighter's mission or the concept of operations²⁷. For more information, see Rapid Prototyping Section C.1.1.

C.2 Agile Development and Development Security Operations (DevSecOps) Programs

Agile software development practices integrate planning, design, development, integration, and testing into an iterative lifecycle to deliver software at frequent intervals²⁸. Programs use Agile software development frequent iterations (also known as sprints) to measure capability development progress, reduce technical and programmatic risk, and respond to feedback and changes more quickly than using traditional methods. Cyber T&E is an ongoing process integrated with the Agile development process influencing both Network Operations and Security Operations. Cyber T&E within Agile uses a continuous feedback process to provide continuous incremental product improvements including the security posture of the product, while assessing the program's path to meeting the System Survivability KPP, if applicable, through the programs lifecycle. Figure C-3 illustrates continuous T&E in the Agile software development process.

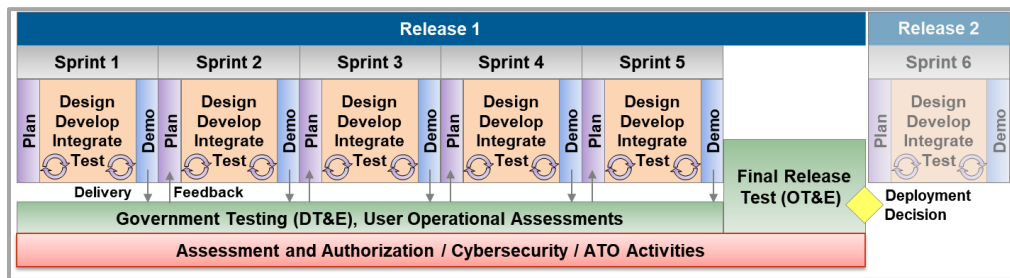


Figure C-3. T&E During Agile Software Development

In DevOps the traditional software development lifecycle waterfall development process is replaced with small but more frequent deliveries²⁹. Each small delivery is accomplished through an automated process or semi-automated process with minimal human intervention to accelerate continuous integration and capability delivery³⁰. DevOps is not Agile software development, but Agile techniques can be used to feed new code and functionality into DevOps. DevSecOps is a DevOps process where Security (Sec) is considered in system planning, architecture and design, and throughout the entire DevOps process. DevSecOps shifts cybersecurity testing to the left by embedding security testing tools and processes in the

²⁷ DOT&E. Operational and Live-Fire Test and Evaluation Planning Guidelines for Middle Tier of Acquisition Programs, October 24, 2019

²⁸ MITRE, *Defense Agile Acquisition Guide*, March 2014

²⁹ DoD CIO, *DoD Enterprise DevSecOps Reference Design*, Version 1.0 12 August 2019

³⁰ Ibid

software development and release processes to create a continuous, integrated process³¹. Figure C-4 illustrates this concept for the DoD.

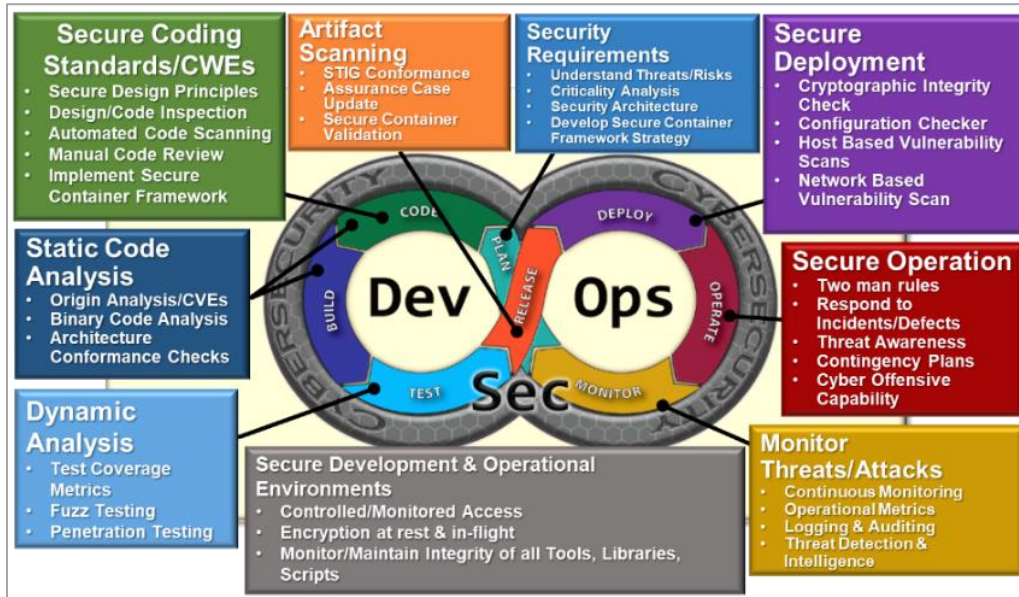


Figure C-4. The Sec in DevSecOps³²

For DoD DevSecOps processes, CDTs and T&E Leads should verify in the contract and ensure that the contractor establishes and maintains a secure development environment, and secure developmental test and pre-production test environments. Multiple secure test environments mimic the production environment to facilitate continuous cybersecurity T&E for software from coding through to production as each capability increment moves through the process. This automated, continuous, contractor testing during small capability increments is what reduces the need for government security acceptance testing to rapidly field new capabilities. Without continuous security testing during system development, shortened test cycles are not possible.

Programs should ensure that government testers can audit the contractor development facilities to ensure that automated security testing is in fact occurring during the software development process. Programs should also ensure that the development environment is secure and free from compromise by adversaries while software development is occurring. Programs should request via development contracts and then verify that the development environment is staffed by known, vetted, trusted personnel, and uses secure, malware-free tools, libraries and scripts. For more information about system development contracts, refer to Appendix B of this Guidebook. Cybersecurity test considerations for DevSecOps include:

- The CyWG is ongoing and MBCRAs recur in synchronization with the Agile development process, as described in the main sections of this guidebook
- Phase 1 and 2 analysis provide continuous feedback into the Agile process for product improvement over time. Analysis of requirements, changes in product architecture (Phase 1) and evolving cyber threats (Phase 2) require repetitive assessment of threat vectors and corresponding

³¹ Ibid

³² Tim Stark. *Recommendations for DevSecOps in Real-Time (RT), Embedded, Critical Systems*, presentation to DDR&E June 4, 2019

adjustments to the cyber test strategy to maintain system cyber survivability and operational resilience.

- Scheduling Phase 3/4 testers on a recurring date-based frequency may be more efficient than capability delivery-based scheduling
- Contractor pipeline of acceptance criteria and test tools' objectives should be thoroughly understood and compared to DoD cybersecurity requirements
- Minimal Viable Products (MVPs) should undergo system cyber survivability and operational resilience testing
- The contractor's test results should be made available to the government

Analysis: Phases 1 and 2 –Testers examine the system security architecture and the planned secure software development factory including tools, processes and personnel vetting processes. Assessment of the development environment during Phases 1 and 2 informs the initial government authorization to the contractor to proceed to system development. Phase 1 and 2 analysis is repeated for each set of new capability.

Integrated Contractor-Government Testing: Early Continuous Phases 3 and 4 - While Figure C-4 depicts testing as a single phase, actual security testing occurs continuously in each phase and is performed as a continuous part of system development. Government testers may be embedded in the contractor developmental test activities. Below are examples of contractor testing activities by DevSecOps process phase. For more information about DevSecOps testing processes for contractors, refer to *DoD Enterprise DevSecOps Reference Design, Version 1.0, 12 August 2019 published by the DoD CIO*. Programs should request that contractors perform the following security tasks during system development:

Secure System Development – Integrate continuous security assessment during development using a secure development test environment.

- Use test tools to scan and analyze the code as the developer writes it to notify developer of potential code weakness and suggest remediation. Monitor the development environment for malicious activity.³³
- Monitor source code repositories for suspicious content such as Secure Shell (SSH) keys, authorization tokens, passwords and other sensitive information before pushing the changes to the main repository.³⁴
- Develop detailed test procedures, test data, test scripts, and test scenario configurations for on the specific test tool.³⁵
- Ensure all automated tools used for development and test are the current versions.

Secure System Builds and Pre-release Testing– Test component code and integrated system to prepare for release to user acceptance testing.³⁶

- Conduct Static Application Security Testing (SAST) - SAST analyzes application static code, such as source code, byte code, and binary code, while they are in a non-running state to detect the conditions that indicate code weaknesses. Perform dependency vulnerability checking to identify vulnerabilities in open source-dependent components.³⁷

³³ DoD CIO. *DoD Enterprise DevSecOps Reference Design, Version 1.0, 12 August 2019*

³⁴ Ibid

³⁵ Ibid

³⁶ Ibid

³⁷ Ibid

- Conduct Dynamic Application Security Test (DAST) - DAST analyzes a running application dynamically and identifies runtime vulnerabilities and environment related issues.³⁸
- Conduct Interactive Application Security Test (IAST) - IAST analyzes code for security vulnerabilities while the application is run by an automated test, human tester, or any interacting activity.³⁹
- Conduct manual security tests such as STIG compliance testing, and penetration testing. Penetration testing targets the running application, underlying operating system (OS), and hosting environment.⁴⁰

System Release Testing and System Deployment – Ensure the software/capability baseline remains consistent from development to pre-production testing to production deployment.⁴¹

- Use cryptographic integrity checks to verify that software components that have passed secure build, all tests, and security scans to ensure that the software/capability baselines are not tampered with as they move between environments.⁴²
- Ensure that the pre-production environment precisely mimics the production environment where the capability will be deployed.⁴³

Integrated DT/OT: Phase 3/4/5 - Phase 3/4/5 is integrated government DT/OT that occurs with each release of the software capability to validate product security and secure operations. Testing informs the following milestones:

- **Program Manager Acceptance** - The PM verifies that capabilities delivered during each release meet identified delivery requirements and are ready for formal user testing. Testing is conducted in the developmental test environment. PM Acceptance supports the release proceeding to initial User Acceptance Testing in the developmental test environment.
- **User Acceptance (Pre-Release)** - Operational users ensure that delivered capability fulfills the functionality requirements identified for the capability release. Testing is conducted in the developmental test environment. Successful testing supports the capability release proceeding to User Acceptance Testing in the operationally representative test environment.

Integrated DT/OT Phase 3/4/5: Prototyping phase: Mature prototypes can conduct a contractor or government cyber DT/OT to assess the products cybersecurity Technology Readiness Level (TRL), as well as mitigating risk in support of obtaining an Authority to Operate (ATO). Agile development enables the development of early prototypes. As product maturity increases, including the execution of the RMF process, PMs can begin early assessment of the product to determine pre-MS-B readiness.



OT CVPA and AA: Phase 5/6 - Government adversarial test teams conduct AA testing in the operational, production environment from the standpoint of a cyber adversary. The OTA will consider applicable information from completed testing when identifying and planning the events needed for the CVPA and AA. Testing informs the following milestones:

- **User Acceptance (Release)** - Operational users ensure that delivered capability fulfills the functionality requirements identified for the functional release in the operational (or operationally representative) environment while maintaining overall system cyber survivability. Successful testing supports the capability release to the operational community.

³⁸ Ibid

³⁹ Ibid

⁴⁰ Ibid

⁴¹ Ibid

⁴² Ibid

⁴³ Ibid

C.3 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 programs (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.

Analysis: Phase 1 and 2 – 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. If multiple software releases to end users create new requirements, consider repeating Phase 1 and 2. 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.



Integrated Contractor-Government Testing: Phases 3 and 4 - If the contractor is required to perform Phase 3 testing and the test results are sufficient, the system could move directly into acceptance testing in the operational environment.

Integrated DT/OT Phase 3/4/5 - Cybersecurity DT&E iteratively performs acceptance testing of implemented security controls and performance parameters to find and fix vulnerabilities before the formal security controls assessment. This process provides test data that satisfies RMF requirements. The combined events occur before initial fielding. PMs should 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).



OT CVPA and AA: Phase 5/6 - Government testers should conduct both the CVPA and AA depending on Phase 1 and 2 analyses and the results of the Phase 3/4/5 Integrated DT/OT. The testing should be performed in the operational, production environment.

C.4 DoD Cloud Computing Platforms

For more information on cybersecurity testing of cloud computing platforms, including the shared security model and specific considerations for testing commercial cloud deployments, refer to the *Cloud Cybersecurity T&E Addendum*.

The Federal Risk and Authorization Management Program (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)⁴⁴ 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 Offerings (CSOs) such as Infrastructure-as-a-Service, Platform-as-a-Service or Software-as-a-Service 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 and covers several areas:

⁴⁴ DISA. Department of Defense (DoD) *Cloud Computing Security Requirements Guide (SRG)* Version 1, Release 1 (12 January 2015)

- Security requirements for CSPs’ cloud service offerings.
- Security requirements for assessing commercial and DoD CSPs for inclusion in the DoD Cloud Service Catalog.
- Security requirements for Mission Owners’ 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 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 conducted 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.

C.5 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.

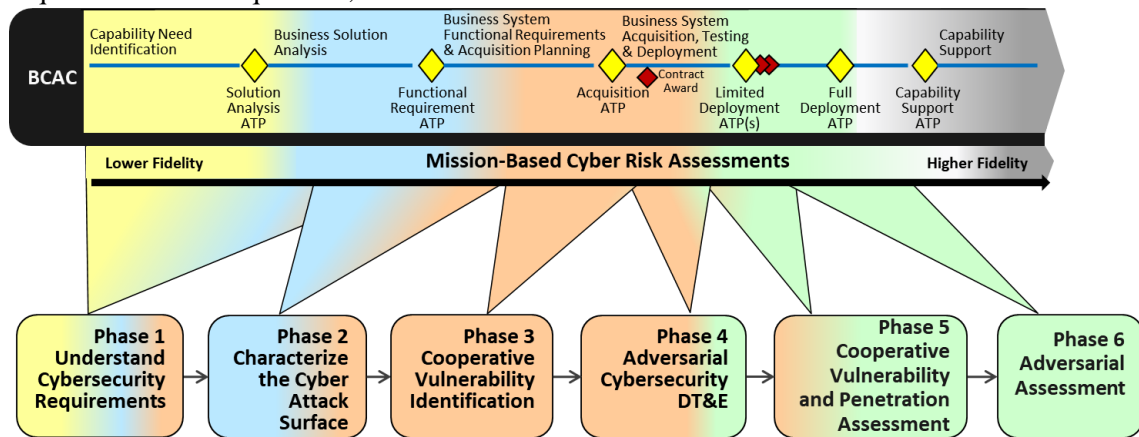


Figure C-5 shows the cybersecurity T&E process mapped to the BCAC process.

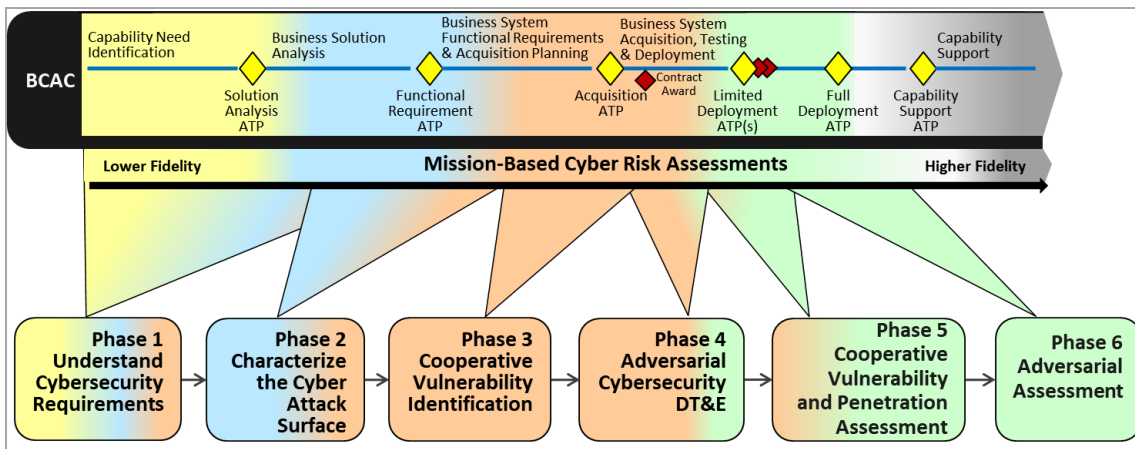


Figure C-5. Cybersecurity T&E Phases Mapped to the BCAC Process

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 Memorandum – 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-1 shows the BCAC acquisition decisions informed by cybersecurity T&E.

Table C-1. BCAC Acquisition Decisions Informed by Cybersecurity T&E

Cybersecurity T&E Functions	Cybersecurity T&E Phase	DoDI 5000.75 Decision and Review Points Influenced
Early Cybersecurity Tester Involvement Activities	Phase 1	BCAC Solution Analysis ATP and Functional Requirements ATP
DT&E/OT&E Planning Activities	Phase 2, 3	BCAC Functional Requirements ATP, Draft RFP, Acquisition ATP
DT&E Test Execution Activities	Phase 3, 4	BCAC Limited Deployment ATP(s)
OT&E Test Execution Activities	Phase 5, 6	BCAC Full Deployment ATP;

Requirements and Attack Surface Analysis – DBS’ programs share some characteristics with software intensive systems due to using COTS products. If DBS programs select a COTS solution, cybersecurity testers should conduct Phases 1 and 2 analyses to inform the ATPs shown in Table C-3. Phase 1 and 2 analyses may rely heavily on RMF artifacts. It may be possible to merge Phases 1, 2, and 3 by 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 that documentation and tracking of vulnerabilities and use publicly available vulnerability databases to ensure discovery and remediation of known vulnerabilities prior to system deployment.

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.

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 should 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 should 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 (CSE IG) – 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 CSE IG provides the guidance for developing the CSRC contained in the acquisition program’s CDD and other requirements documents. Acquisition programs should refer to the CSE IG 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 operational resilience requirements, approach, testing,

deficiencies, 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 IT 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 Plan - Operational Test Plans are key artifacts for OT&E of Phases 5 and 6. Operational Test Plans contain cybersecurity test objectives, measures, activities, and test resources that are approved by DOT&E no later than 60 days prior to commencement of testing. Test plans contain details of how the OTA will test to provide the required cybersecurity data including resources, schedule, OTA-specific test and data collection tools, and data to be collected. For more information about Operational Test Plans see DOT&E Memorandum, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs,” April 3, 2018

Operational Test Readiness Review (OTRR) – The OTRR is a service-specific multi-disciplined product and process assessment to ensure that the system can proceed into Initial Operation Test and Evaluation (IOT&E) with a high probability of success, and that the system is effective and suitable for service introduction. Services with OSD T&E oversight list programs are required by DoD policy to establish a Service process for determining and certifying a program’s readiness for IOT&E by the Service Component Acquisition Executive (CAE).The OTRR may be conducted by the Program Manager or the Operational Test Agency, depending on Service policy. (Source: DAU)

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.

RMF 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.



RMF Security Plan – The RMF Security Plan is reviewed as part of the first phase of cybersecurity T&E to assist in understanding cybersecurity and operational 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.



RMF 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.

System Requirements Document (SRD) – The 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.

Test & 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 activities, and provides a clear roadmap connecting evaluation objectives, test measures, requirements, test methodologies, decision points, test events, and resources.

Validated On-Line Lifecycle 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.

Appendix E Guidance for the Cybersecurity Portion of the Developmental Evaluation Framework (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 Decision Support Questions (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, should 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
- System cyber survivability and operational resilience
- 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.

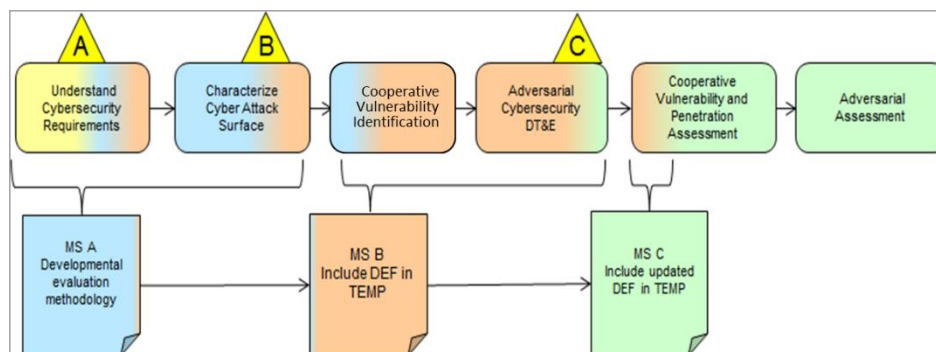


Figure E-1. DEF Schedule

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, and 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. Data security both within the system boundary and across interfaces and system or mission operational resilience 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

Developmental Evaluation Objectives	System Requirements / Measures		Decision #1		Decision #2			Decision #3	Decision #4	
			DSQ #1	DSQ #2	DSQ #3	DSQ #4	DSQ #5	DSQ #6	DSQ #7	DSQ #8
Functional evaluation areas System capability categories	Technical Reqmts Document Reference	Description	Data Sources (Test, M&S events)							
Performance										
Performance Capability #1	3.x.x.5	Technical Measure #1	DT #1		M&S #2				DT #4	M&S #2
	3.x.x.6	Technical Measure #2	M&S #1		DT #3				DT #4	M&S #2
Performance Capability #2	3.x.x.7	Technical Measure #3				DT #3		IT #1		
	3.x.x.8	Technical Measure #4				M&S #4		IT #1		
Interoperability										
Interoperability Capability #1	3.x.x.1	Technical Measure #1				DT #3		DT #4		
Interoperability Capability #2	3.x.x.2	Technical Measure #2		IT #2		M&S #4		DT #4		M&S #2
	3.x.x.3	Technical Measure #3		IT #2				IT #1		DT #3
Cybersecurity										
Security Capability #1	5.x.x.1	Technical Measure #1	CTT #1				CVI #2	ACD	CVI #3	
	5.x.x.2	Technical Measure #2	CTT #1			SCA		ACD	CVI #3	
Security Capability #2	5.x.x.3	Technical Measure #3		CVI #1		SCA		ACD		ACD
	5.x.x.4	Technical Measure #4	CTT #1		CVI #1			ACD	CVI #3	
Reliability										
Reliability Capability #1	4.x.x.1	Technical Measure #1		M-demo #1						IT #5
	4.x.x.2	Technical Measure #2		M-demo #1				IT #2		IT #5
Reliability Capability #2	4.x.x.3	Technical Measure #3				M-demo #2		IT #2		
	4.x.x.4	Technical Measure #4				M-demo #2		IT #2		

Figure E-2. Developmental Evaluation Framework Format

E.4 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 that 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 decision makers need 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 operational 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 resilience and survivability.

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

cyber survivability and operational resilience. 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 Task 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 should 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 Task 3.

Task 4 of the cybersecurity DEF engagement is to include the DEF in 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.

Developmental Evaluation Objectives	System Requirements/ Technical Measures	EMD RFP Release	EMD Long Lead Items for A/C (A1, A2, A3) & Radars (for A/C and SIL)	MS B / Contract Award	Approval to Enter Gov't Lead IDT&E	LRIP Long Lead Items	Approval to Enter IOT&E
System Capabilities	SRD Rqmt's (Potential CTPs*)	DSQ1: Did at least two contractors provide technical designs and information for successful PDRI's?	DSQ2: Have at least two contractors demonstrated sufficient subsystem maturity?	DSQ4: Can the Radar and SUT subsystem integration meet Performance and Processing Requirements?	DSQ5: Has the KTR demonstrated a fully integrated, functional and stable, Radar/Comm/ C2 capability in the SIL?	DSQ7: Do any system deficiencies preclude an LRIP purchase?	DSQ8: Does the performance and reliability support all required mission profiles?
		Technical Measures	DSQ3: Can the Aircraft meet Requirements?	DSQ6: Has the KTR demonstrated a fully integrated, functional and stable, Radar/Comm/C2 system?	DSQ9: Are cybersecurity vulnerabilities identified and acceptable mitigations in place?		
Protect: Data Security - System	Data at rest, Data in transmission	Architectural Vulnerability Analysis (AVA)	Mission Cyber Dependency Analysis - Cyber Table Top Exercise	CVI - Data Security testing CVI-STIG compliance verification	Security Controls Assessment (SCA)		
		Software Assurance	Contractor T&E	CVI - Software Development Verification			
		Supply Chain Risk Management	SCRMM TAC Assessment	SCRMM TAC Assessment	SCRMM TAC Assessment		
Protect: Data Security - Interfaces	Hardware Assurance	Architectural Vulnerability Analysis (AVA)	CVI - Hardware Development Verification	CVI - Hardware Development Verification			
		Critical Data Exchanges	Architectural Vulnerability Analysis (AVA)	Interoperability - Cybersecurity/IT			
		Detecting attacks (how long to detect, how many detected versus attempted, mission impacts)	Mission Cyber Dependency Analysis - Cyber Table Top Exercise	CTT Verification Exercise	CTT Verification Exercise	ACD	
System Resilience and Survivability	SS KPP CSA	Responding to attacks (how long to respond)	Mission Cyber Dependency Analysis - Cyber Table Top Exercise	CVI - Cyber Functionality Verification	CVI - Incident Response Assessment	ACD	ACD
		Recovering from attacks (how long does recovery take? Does that impact success of the mission?)	Mission Cyber Dependency Analysis - Cyber Table Top Exercise	CVI - COOP assessment	CVI - COOP assessment	ACD	ACD

Figure E-3. Example DEF Completed Cybersecurity Section

E.7 Cyber Portion of the DEF for Agile System Development

Agile development processes (Agile) integrate planning, design, development, and testing into an iterative lifecycle to deliver software at frequent intervals. Programs using Agile development techniques can tailor the DEF for their systems even though Agile software development programs do not typically follow DoDI 5000.02 acquisition timelines. With Agile, program managers should be concerned with whether previously identified issues are addressed when determining if a capability should be released in its current form. Below is an example of high-level acquisition decisions that may be supported by cybersecurity testing:

- Initial Authorization to Proceed to Development – Conducted as an assessment of the development environment
- Program Manager Acceptance - Verifies that capabilities delivered during each release by the implementer meet identified delivery requirements and are ready for formal user testing. Testing is conducted in the developmental test environment. Decision supports the release/functional drop proceeding to initial User Acceptance Testing in the developmental test environment
- User Acceptance (Phase 1) - Operational users ensure that delivered capability fulfills the functionality requirements identified for that functional release. Testing is conducted in the developmental test environment while maintaining overall system cyber survivability. This acquisition phase supports the capability release proceeding to User Acceptance Testing in the operationally representative test environment.
- User Acceptance (Phase 2) - Operational users ensure delivered capability fulfills the functionality requirements identified for the functional release in the operational (or operationally representative) environment while maintaining overall system cyber survivability. Decision supports the capability release to the operational community.
- Authorization to Proceed - Testers periodically (e.g., annually) verify that all system capabilities deployed to date can support the mission in the operational environment when subjected to operationally representative cyber threats. This phase also verifies that the development environment is still operationally representative, cyber-secure, and meets ATO/development requirements (e.g., identifies and evaluates any changes in development environment since previous assessment and approval).

Figure E-4 shows how these acquisition decisions can be tailored in the Program's DEF.

Developmental Evaluation Objectives	Initial Authorization to Proceed to Development		Program Manager Acceptance		User Acceptance (Phase 1)		User Acceptance (Phase 2)		Periodic Authorization to Continue Development						
	Prior to Initial System Development		Each Release		Each Release		Each Release (as required)		Periodic						
System Requirements/Measures	DSQ 1: Is the Developmental Environment accessible by integrated government test agencies?	DSQ 2: Is the Developmental Environment accessible by integrated government test agencies?	DSQ 3: Are the requirements allocated to the release satisfied?	DSQ 4: Is the system interoperable?	DSQ 5: Have critical functionality concerns been corrected or mitigated?	DSQ 6: Are the requirements allocated to the release satisfied?	DSQ 7: Is the system interoperable?	DSQ 8: Have critical functionality concerns been corrected or mitigated?	DSQ 9: Are the requirements allocated to the release satisfied?	DSQ 10: Is the system interoperable?	DSQ 11: Have critical functionality concerns been corrected or mitigated?	DSQ 12: Are requirements allocated to all releases to date satisfied?	DSQ 13: Is the system interoperable?	DSQ 14: Have critical functionality concerns been corrected or mitigated?	DSQ 15: Is the Developmental Environment representative?
Functional Evaluation Areas	Technical Requirements (Document Reference)	Description	Data Sources												
Data Security	DODI 8510; PPP	System prevents loss of data confidentiality	Dev STIG verification, MB CRA									Dev STIG verification, Platform and Component Hardening, MB CRA			
	DODI 8510; PPP	System prevents loss of data integrity	Platform and Component Hardening, MB CRA									Platform and Component Hardening			
	DODI 8510; PPP	System prevents loss of data availability	Security Controls Assessment, MB CRA									Security Controls Assessment			AVA, SW Testing - Dev Environment
Operational Resilience and System Survivability	SS-KPP, DODI 8530, 8500	System prevents cyber intrusions from negatively impacting mission effectiveness/mission functions	AVA informed testing Cybersecurity Functionality Verification												
	SS-KPP, DODI 8530, 8500	System mitigates the effects of cyber-attacks, enabling the system to complete critical mission tasks	AVA informed testing	SW Testing - Operational Release, Misuse/Abuse Testing											
	SS-KPP, DODI 8530, 8500	System is able to recover from cyber-attacks and restore full functionality quickly	AVA informed testing	Cyber Functionality Verification, CVI Penetration Testing, MB CRA											

Figure E-4. Cyber Portion of the DEF for Agile Development Process

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 should 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 and 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 should 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 standards, system cyber survivability and operational resilience 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 Program Executive Office
- 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 federally funded research and development center (FFRDC) and/or university affiliated research center (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 analyzing, planning and conducting cybersecurity T&E activities. Cybersecurity T&E

technical experts include hands-on testers, analysts, assessors and SMEs in a variety of technical disciplines. The following section describes the roles typically needed to plan and conduct cybersecurity 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 that 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, or 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 operational resilience and system cyber 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 that 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 that the event and report data are handled at the appropriate level if defined in a Security Classification Guide
- 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 qualifications⁴⁵:

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

⁴⁵ 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 [TCP] and Internet Protocol [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 should generate and how to analyze the 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 control 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 should 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, research and development (R&D) organizations, vendors, national laboratories, and other services. It is important for cybersecurity SMEs to work closely with operational SMEs who thoroughly know the system from a design, functional and operational standpoint. These SMEs should participate in Phase 1-6 activities.

Software assurance testing SMEs specialize in testing software at the code level and can examine code for code-based vulnerabilities. Software assurance testing SMEs also can recommend test tools specific to software testing such as static and dynamic test tools.

Cybersecurity SMEs - Recommended Minimum Qualifications. The SMEs and 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 Cybersecurity T&E Leads for Cybersecurity Developmental Testing

For Phases 1-4, the Lead Developmental Test Organization or the system's government cybersecurity DT&E organization that is resourced for cybersecurity DT&E, should provide a Cybersecurity 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 standards, operational resilience and system cyber survivability. The Cybersecurity T&E Lead should plan government cybersecurity test events by recruiting the staff needed to support events, developing test plans and documenting test results in reports. The Cybersecurity 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 Cybersecurity T&E Event Lead (contractor, government, range) is responsible for leading the team of testers executing each event. The Cybersecurity T&E Lead and the Cybersecurity T&E Event Lead work together in executing all developmental test events.

The DoD Cybersecurity T&E Cross-Service working group has recommended a set of qualification standards expressed as knowledge, skills, and abilities (KSAs) for Cybersecurity T&E Leads that includes technical and leadership skills. For more information, refer to *Cybersecurity Vulnerability Analysis Standards*.⁴⁶

F.2.1.4 Cybersecurity Vulnerability Analysts

Cybersecurity Vulnerability Analysts (VAs) are hands-on testers who use both automated tools and manual 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. Cybersecurity 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 DoD Cybersecurity T&E Cross-Service working group has recommended a set of KSAs and a progression of knowledge for Cybersecurity VAs.⁴⁷ The standards allow organizations to train and develop their workforce to support cyber DT events that align with cybersecurity T&E Phases 1 to 4 of the acquisition lifecycle. Program and Service-specific complementary requirements may be used in addition to these standards. VAs are beneficial at different proficiency levels and the VA standards describe a career progression from apprentice to master VA and lead VA. Figure F-1 shows this progression.

⁴⁶ Cybersecurity Vulnerability Analysis Standards, OUSD(DT&E)

⁴⁷ Ibid

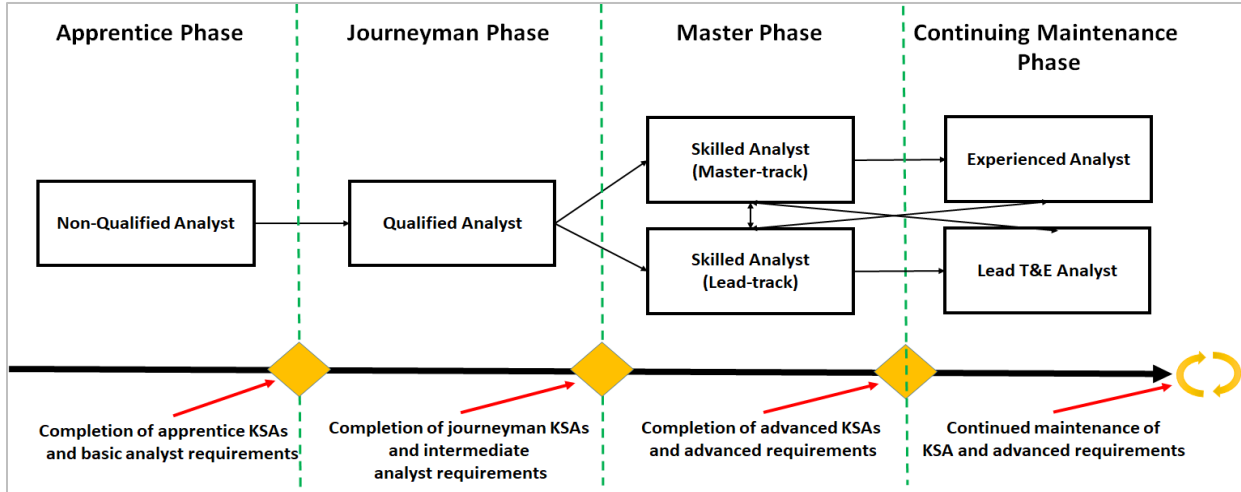


Figure F-1. Vulnerability Analyst Proficiency and Maturity Levels

For more information, refer to *Cybersecurity Vulnerability Analysis Standards*.⁴⁸

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 should 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 Tester⁴⁹:

- At least three years of related cybersecurity experience
- Familiarity and experience with common 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
- Familiarity with cybersecurity defenses (Intrusion Prevention System/Intrusion Detection System, 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

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

⁴⁸ Cybersecurity T&E Cross Service Working Group. *Cybersecurity Vulnerability Analysis Standards*.

⁴⁹ Ibid

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) may be certified by the NSA and accredited through U.S. Cyber Command (USCC) to ensure they are able to transit DoD networks without doing harm to government systems. CJCSM 6510.03 describes Red Team certification and accreditation. Note that NSA/USCC certification is not required for all Red Team organizations.

Red Team Testers - Recommended Minimum Qualifications. As with the Cybersecurity SMEs and the Cybersecurity VAs, Red Team testers should have prior experience with the protocols, architectures, networks and interfaces associated with the systems under test. Their minimum qualifications are similar to PAT 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. The Cyber Test Range Representatives possess analysis skills and test skills in the areas of penetration testing and adversarial testing to support cybersecurity test planning. This includes a variety of skills and expertise, including knowledge of distributed testing, virtual environment emulation, network engineering, 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 that cyber range capabilities meet their requirements. The Event Planner/Coordinator participates in event planning milestones and coordinates with all other planning roles to ensure that required capabilities are provisioned for test events.⁵⁰

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 health and status monitoring required throughout the test event.⁵¹

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.⁵²

Security Engineer – Personnel who monitor, manage, and configure security devices and controls associated with cyber range events.⁵³

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 cybersecurity 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 Test Resource Management Center (TRMC) to support the planning, execution, and analysis of test and training events. The 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:

⁵⁰Adapted from DoD OSD/AT&L, DASD DT&E/TRMC, *The Cyber-Range Event Process*, Version 1.0 (January 2015)

⁵¹ Ibid

⁵² Ibid

⁵³ Ibid

- 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, facilities and 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 Qualifications⁵⁴:

- 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

F.3 Cybersecurity Roles and Responsibilities – RASCI

As discussed briefly in Section 3.2 of this guidebook, each Program Office should convene a 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 Responsible, Accountable, Supporting, Consulting, Informed (RASCI) matrix listing the various personnel and their appropriate RASCI for each task. Figure F-2 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.

⁵⁴ Adapted from Naval Air Systems Command, *Standard Work Package for Cyber Developmental Testing & Evaluation* (2016 July 28)

Example Cybersecurity Working Group Roles	Chief Developmental Tester	Systems Security Engineer	Information Systems Engineer	Lead Systems Engineer	Lead Software Engineer	Lead DT&E Organization	Operational Test Agency Representative	Cybersecurity DT&E Representative	Cybersecurity OTA Technical Experts	Security Controls SMEs	Cybersecurity SMEs	CS&P/DCO Representative	System Maintainer / Logistics	Cyber Test Range Representative	Service T&E Policy Representative
	R=Responsible, A=Accountable, S=Supporting, C=Consulting, I=Informed														
Major Cybersecurity Tasks															
Phase 1	Understand Cybersecurity Requirements (and Plan for T&E)														
Compile List of Cybersecurity and Resiliency Requirements	A	S	S	C	C	R	C	S	C	S	S	C	C	C	I
Prepare for Cybersecurity T&E Events	A	S	S	C	S	S	S	R	R	S	S	C	C	C	S
Develop Cybersecurity T&E Strategy	A	S	S	C	C	R	R	S	S	S	C	C	C	C	I
Phase 2	Characterize the Cyber-Attack Surface														
Identify the Cyber-Attack Surface	A	S	S	C	S	C		R	S	S	S	S	S		I
Analyze the Cyber-Attack Surface	A	S	S	C	S	C		R	S	S	S	S	S		I
Document Analysis Results and Update Test Plans	A					C		R	S	S		I	I	I	I
Prepare for Phase 3 and 4 Cybersecurity T&E Events	A	S				R		S	S	S		I	I	I	S
Phase 3	Cooperative Vulnerability Assessment (CVI)														
Plan CVI Test Activities	A	S				R		S		S	C	S	I	I	S
Conduct CVI Events	A	S				R		S		S	C	S	I	I	S
Document CVI Test Results	A	S				S		R		S	C	I	I	I	I
Prepare for Phase 4 Cybersecurity T&E events	A		S					S		C	C	S	I	I	S
Phase 4	Adversarial Cybersecurity DT&E (ACD)														
Update Cyber Threat Assessment	A	S	S	S	S	R		S			S	S			I
Update Kill Chain Analysis	A	S	S	S	S	C	R			S	S	S			I
Plan Adversarial DT&E	A		S			C		R		S	S			S	I
Conduct ACD	A		S			S		R		S	S	S	S	S	I
Document ACD Test Results	A	I	S	I	I	S		R	I	I	S	S	S	S	I
Phase 5	Cooperative Vulnerability and Penetration Assessment (CVPA)														
Plan CVPA			S					A		R		S	S	S	C
Coordinate with Cybersecurity Vulnerability Assessment Team			S					A		R		S	S	S	C
Execute CVPA and Document Results			S					A		R		S	S	S	C
Phase 6	Adversarial Assessment														
Plan Adversarial Assessment			S					A		R		S	S	S	C
Coordinate with Cybersecurity Vulnerability Assessment Team			S					A		R		S	S	S	C
Execute AA and Document Results			S					A		R		S	S	S	C

Figure F- 2. 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 accountable for the correct and thorough completion of the deliverable or task, and to whom Responsible is accountable. In other words, an Accountable should sign off (approve) on work that Responsible provides. There should 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, Supporting 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. The DoD Cybersecurity T&E Cross-Service working group has recommended a set of organizational standards to assess whether DT Cyber VA organizations have the administrative capability to support events, are staffed with highly qualified cyber VA personnel, and are committed to the development and retention of their workforce.

Organizational DT Cyber VA standards ensure that organizations are equipped to conduct cyber vulnerability assessments and analyses across cybersecurity T&E Phases 1 through 4. The list below summarizes the organizational qualification standards to support cybersecurity T&E.

- Professional Development - The organization possesses a funding line to provide formal industry vendor training, develops and maintains in-house training that is specialized and targeted to customer mission space, has the capability for participation in R&D/Science and Technology innovation projects to support cyber vulnerability analysis and assessments, is an active participant in Joint cybersecurity VA training exercises, and provides cyber SME workforce career advancement opportunities for formal education, temporary assignment rotations, and the Defense Acquisition University (DAU).
- Cyber VA Tools - The organization has the resources and capacity to develop custom mission-based cyber VA tools, techniques and methodologies; the configuration management processes, procedures, and infrastructure for cyber VA tools; and appropriate documentation for the use of developed cyber VA tools.
- Laboratory and Facilities - The organization maintains laboratory facilities, environments, infrastructure (i.e., virtual environment and capabilities) and network connectivity aligned to customer and cybersecurity T&E mission/technology to facilitate professional development.
- Human Capital - The organization has processes and procedures as part of their hiring plan to hire qualified cyber SMEs and provides opportunities to incentivize and retain cyber workforce.
- Procurement - The organization has a funding line to procure equipment and services to support cybersecurity T&E workforce maintenance and development.
- Work Products Standards (Test Plan) - The organization has capacity to staff test plans in support of cyber VA events. They should provide a test plan containing (but not limited to) the following required sections: Rules of Engagement (ROE), Cyber VA Methodology and Tools, System Characterization, Characterized Attack Cyber-Attack surface and Attack Vectors, and event constraints and limitations.
- Work Product Standards (Final Report) - The organization has capacity to staff Cyber VA technical reports and ensure that the report includes the following required information: evidence of confirmed cyber vulnerabilities, Cyber VA risk assessment mitigation, and risk management recommendations.
- Legal Review Process - The organization has an internal legal review process to cover approval of all standard (template) test plans, standard operating procedures (SOPs), and ROEs and respond to test critical questions or issues within 48 hours for any Cyber VA event.

- Threat Intel Community Relationship - The organization has established relationships with the threat intelligence community to include organizations that provide current threat information and participation in working groups bi-annually at minimum.
- Standard Operating Procedures - The organization possesses a baseline set of SOPs) in support of cybersecurity T&E that ensure the organization conducts effective planning, execution, and post-analysis of cyber VA events (e.g. emergency halting procedures).

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/>⁵⁵ - Hosted by the Department of Homeland Security (DHS), the NICCS Training Catalog provides a robust listing of cybersecurity and cybersecurity-related training courses offered in the United States. 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 military 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 and 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 should also be identified in either the development or production contract. For more information about TEMP requirements, refer to the DAG, Chapter 8.

F.6 Cybersecurity T&E Organizations

For a current list of T&E organizations, CDTs should refer to DAG, Chapter 8-2.2, 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. Additionally, CDTs can search for cybersecurity T&E organizations, capabilities and tools in the Centralized Cyber Capabilities Directory. More information on the C3D can be requested by emailing c3d-help@ida.org.

⁵⁵ DHS, *National Initiative for Cybersecurity Careers and Studies – NICCS™, NICCS Education and Training Catalog*. <https://niccs.us-cert.gov/training/>

Appendix G Considerations for Software Assurance Testing

The purpose of this Appendix is to ensure that 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 that the software test strategy is properly planned, resourced, and scheduled
- 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 diminishes, confidence increases (both positive and negative) about the software and the test results influence decisions about how to mitigate vulnerabilities that remain.⁵⁶ 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.

⁵⁶ US Department of Commerce, NIST SP 800-160, *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (November 2016).

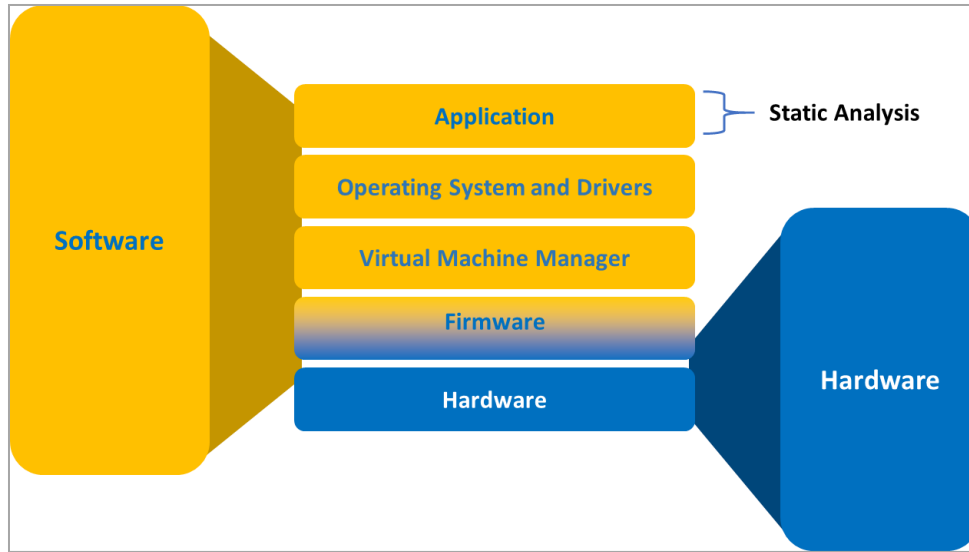


Figure G-1. Software Stack Example

G.2 Software Susceptibility

Coding flaws can lead to vulnerabilities across the entire software stack. The impact of triggering or exploiting vulnerabilities varies from Service/Component to Service/Component and among acquisition programs. For this reason, software testing to achieve enough 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 or 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.

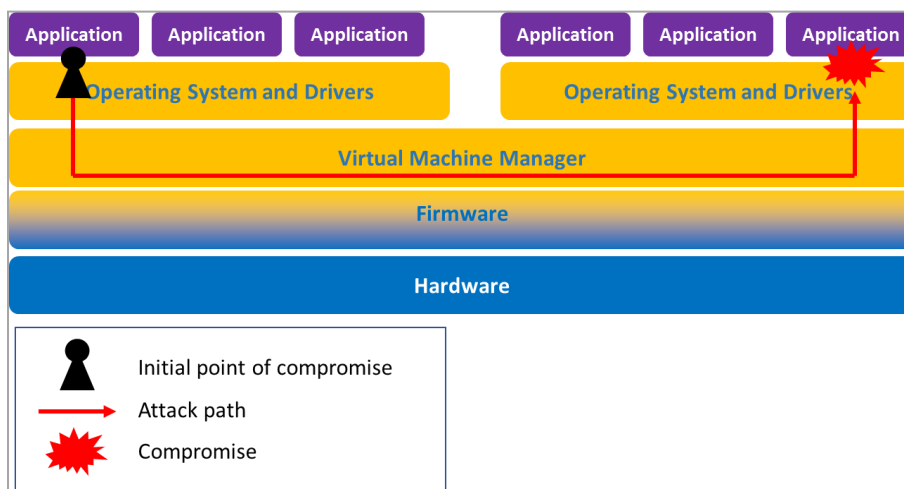


Figure G-2. Compromising the Software Stack

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 Application Programming Interface (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 Basic Input Output System (BIOS)/Unified Extensible Firmware Interface, memory devices, cryptographic key storage, etc. An example of exploiting a vulnerability in firmware is the installation of a BIOS rootkit.

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).

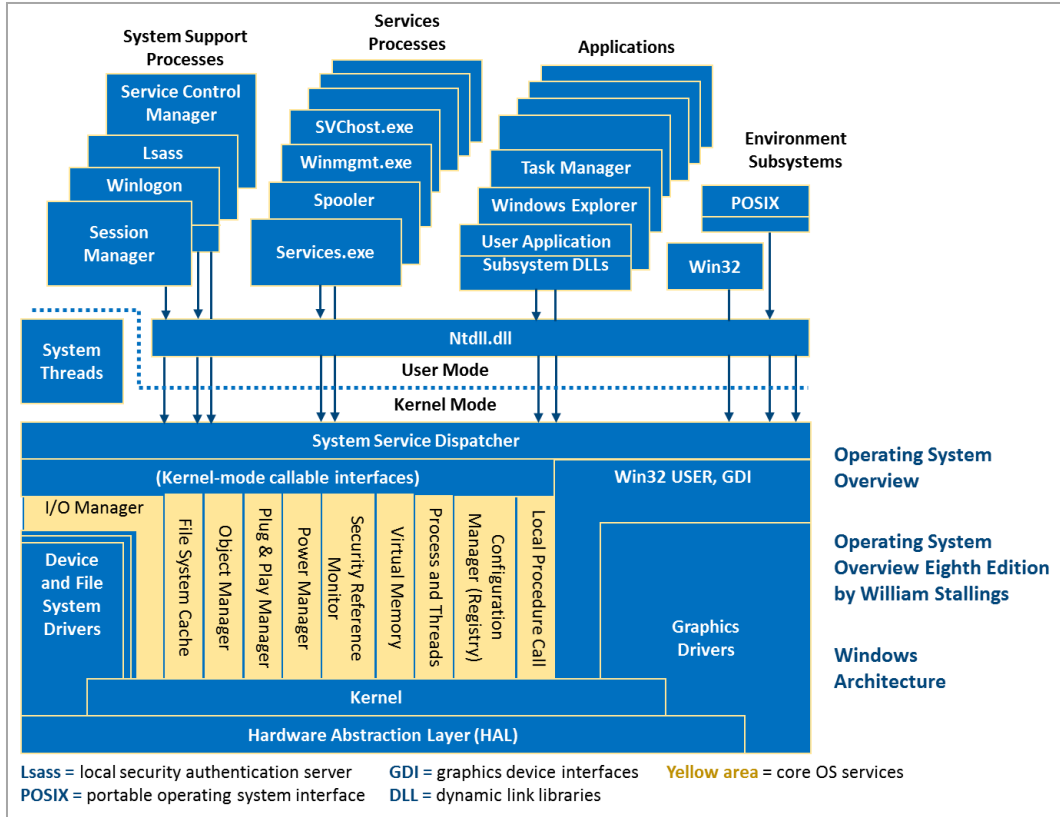


Figure G-3. Windows Architecture⁵⁷

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. A software test strategy can be designed once there is an understanding of the test phases needed as it relates to the component’s software stack.

⁵⁷ William Stallings. *Operating Systems: Internal and Design Principles* 8th edition

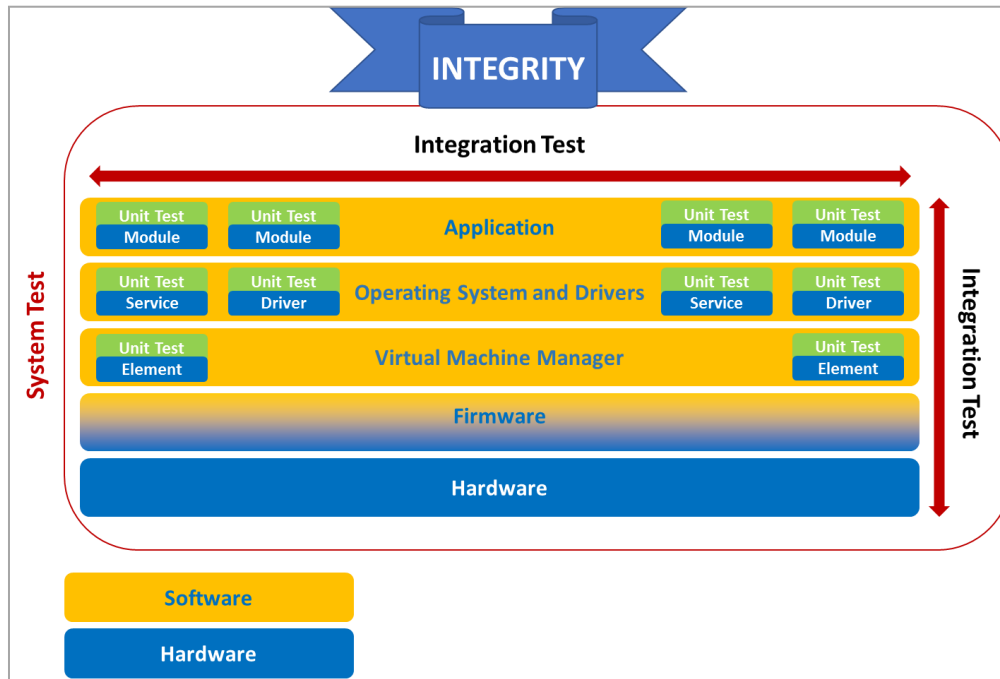


Figure G-4. Software Testing Strategy

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.⁵⁸ 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 identifies errors more readily than 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

⁵⁸ Joint Software Systems Safety Engineering Workgroup. *Joint Software Systems Safety Engineering Handbook*, (2010).

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 that 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.

Resiliency test – Software testing to examine behavior of the software when intentional, unintentional, or malicious activities cause error conditions in the system that could interrupt system operations. Resiliency testing confirms the resilient mechanisms of the software design.

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 should communicate the level of rigor in the software development plan. The contractor should understand the testing rigor the software requires before beginning software development. The RFP, or a controlled source document referenced by the RFP, should include details of design, processes, methods, and tools utilized for testing. These development details should be scrutinized starting with the AoA new capability process. When a new military capability is needed, secure development methods should be available to ensure that the new system, ship, vehicle, or aircraft can remain secure over its life cycle.

To ensure operational security, consider instituting a controlled process of exchanging details on test requirements. For example, if an adversary were to know that 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, system testing, and adherence 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.

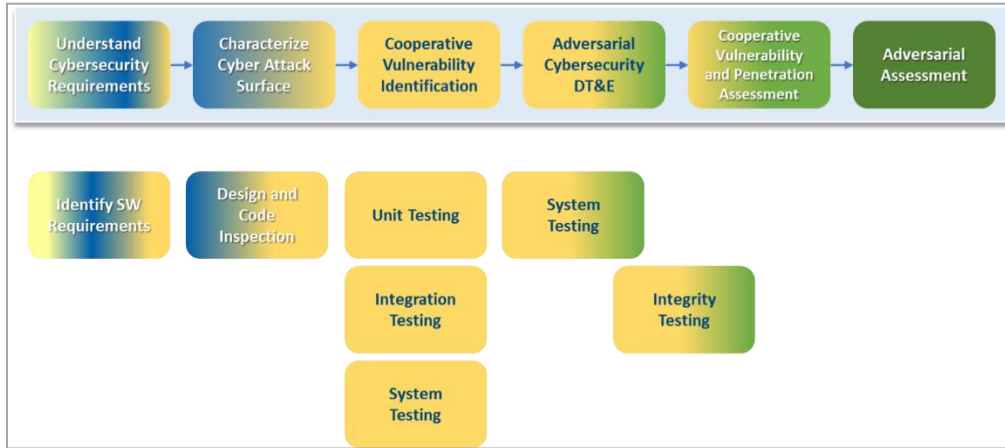


Figure G-5. Software Testing Schedule

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. Testers should revisit requirements as evolving, and new threat information emerges that could result in operational impact. The timing and scope of tests should target the test rigor corresponding with risk acceptance.

Table G-1. Cybersecurity Software Test Requirements

Source	Notionally Implied Cybersecurity SW Test Requirements
PPP	Test requirements confirm: <ul style="list-style-type: none"> • Mitigation of CVEs • Mitigation of common attack pattern enumeration and classification • Mitigation of common weakness enumeration • Effectiveness of fault isolation • Effectiveness of least privilege • Achievement of system element isolation • Input checking and validation measures
TSN	Includes software security focused test requirements in development contracts. Describes contractor software testing activities
STIGs	Confirm compliance with ASD STIG

Source	Notionally Implied Cybersecurity SW Test Requirements
SEP	<ul style="list-style-type: none"> 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

Source	Description
CAPEC	Comprehensive dictionary and classification of know attacks. ⁵⁹
CWE	List of common software security weaknesses. ⁶⁰
CVE	List of common identifiers for publicly known cybersecurity vulnerabilities. ⁶¹
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). ⁶²
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. ⁶³
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 Institute for Defense Analysis publication *State-of-the-Art Resources (SOAR) for Software Vulnerability*

⁵⁹ capec.mitre.org

⁶⁰ cwe.mitre.org

⁶¹ cve.mitre.org

⁶² https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

⁶³ https://attack.mitre.org/wiki/Main_Page

*Detection, Test, and Evaluation 2016*⁶⁴ 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. Static analysis methods may include conducting a CTT that focuses on examining source code, associated mission functions, supply chain interactions, and cyber threats that may exploit vulnerable code.
- **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 10 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*⁶⁵, 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 should determine the sufficient level of rigor needed based on the threats and criticality of the system.

⁶⁴ Institute for Defense Analysis. *State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation (2016)*.

⁶⁵ Ibid. *SOAR Appendix E for Software Vulnerability Detection, Test, and Evaluation (revision 10) Matrix*

Table G-3. Sample Test Methods

Category	Tool/Techniques
Static Analysis	<ul style="list-style-type: none"> • Attack modeling • Warning flags • Source code quality analyzer and source code weakness analyzer • Context-configured source code weakness analyzer • Source code knowledge extractor for architecture/design coding standards – extract design, architecture, mission layer, to aid analysis • Requirements-configured source code knowledge extractor – extract design, architecture, mission layer, to aid analysis • Traditional virus/ spyware scanner • Binary/ bytecode quality analysis • Bytecode weakness analysis - including disassembler + source code weakness analysis • Binary weakness analysis - including disassembler + source code weakness analysis • Inter-application flow analysis • Binary/ bytecode simple extractor – strings, elastic, (ELF readers, etc.) • Compare binary/ bytecode to application permission manifest • Obfuscated code detection • Binary/ bytecode disassembler - then use manual analysis of vulnerabilities and anomalies • Focused manual spot check - focused manual analysis of source • Manual source code review (not inspections) • Inspection (IEEE 1028 standard) (can apply to requirements, design, source code, etc.) • Generated code inspection • Safer languages • Secured library selection • Secured OS • Origin analysis • Digital signature verification • Configuration checker • Permission manifest analysis • Development/ sustainment version control • Obfuscator • Rebuild & compare
Dynamic Analysis	<ul style="list-style-type: none"> • Network scanner - identify (sub)systems & ports • Network sniffer • Network vulnerability scanner – scan for known vulnerabilities for specific products • Host-based vulnerability scanners – examine configuration for flaws, verifying that audit mechanisms work, ensure host configuration meets certain predefined criteria • Host application interface scanner • Web application and web services scanner • Database scanners • Fuzz tester • Framework-based fuzzer • Negative testing – include tests that are supposed to fail due to security mechanisms properly working • Digital forensics • Intrusion Detection Systems/Intrusion Prevention Systems • Automated monitored execution • Forced path execution • Firewall (network and web application) • Man-in-the-middle attack tool • Debugger • Fault injection – source code; Fault injection – binary • Logging systems; SIEM
Hybrid Static/Dynamic Analysis	<ul style="list-style-type: none"> • Test coverage analyzer – statement or branch coverage • Hardening tools/scripts • Execute and compare with application manifest • Track sensitive data • Coverage-guided fuzz tester • Probe-based attack with tracked flow • Track data and control flow

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.

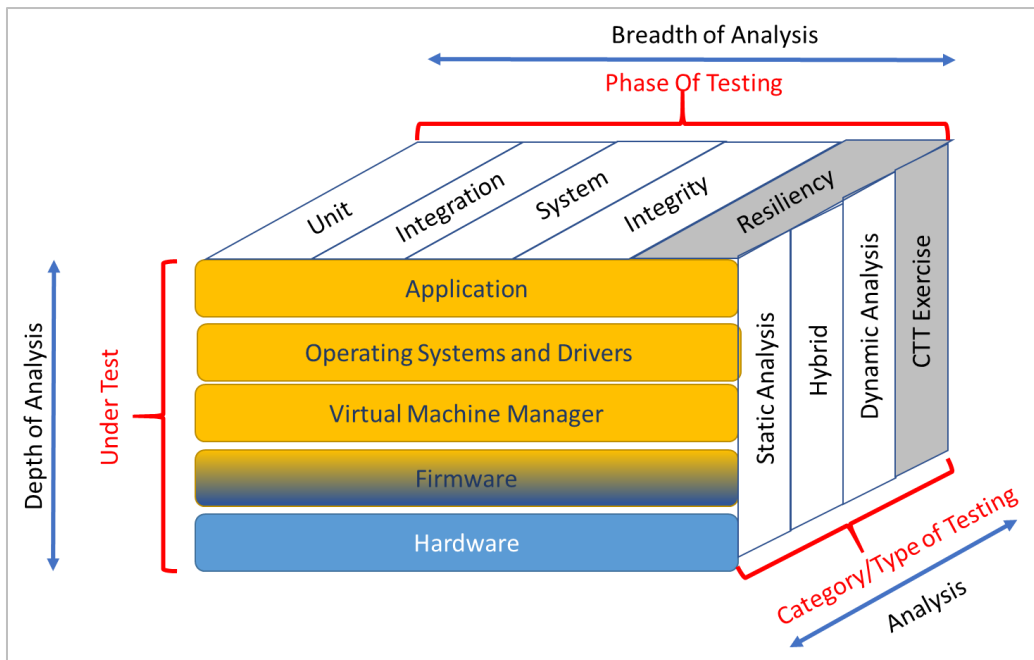


Figure G-6. Testing Rigor

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 that 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 they duplicate every 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.

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 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 reliability⁶⁶. 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 removed⁶⁷. 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 and 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 use profile testing (scenarios) to observe the ability of a system to reconfigure and adapt to change (elasticity) and to adjust and sustain under expected and unexpected conditions (resilience)⁶⁸. This approach requires more maturity, but the models suggested for each of the cyber reliability steps are often practiced in the cybersecurity community.



⁶⁶ Software Engineering Institute. *Predicting Software Assurance Using Quality and Reliability Measures*, (December 2014)

⁶⁷ Ibid.

⁶⁸ IEEE. *Strategy for Reliability Testing and Evaluation of Cyber Physical Systems* (December 2015)

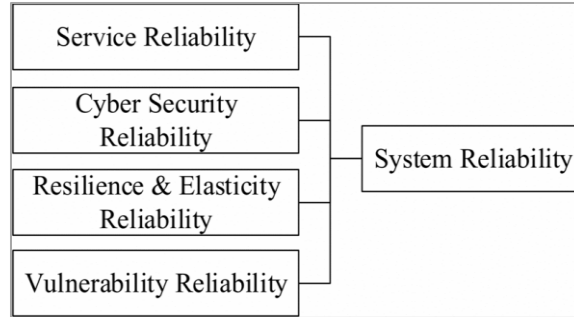


Figure G-7. Comprehensive Evaluation of System Reliability

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, any of the CWEs 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.



Incorporating 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

Trusted System and Network (TSN) Analysis, Appendix A, Part 2⁶⁹ 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)
 - a. 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.

⁶⁹ DASD(SE) and DoD CIO, *Trusted Systems and Networks (TSN) Analysis* (June 2014)

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 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 should reflect software testing activities and include a schedule of assessments (TEMP Part II), resources required for software assessments (TEMP Part IV), and the software T&E tests that occur 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 should 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
- Software testing rigor for inclusion in the Development 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 should explain how the execution of software test activities provide data for evaluations, and how those evaluations provide decision makers with essential

information about the cybersecurity of the software. It should explain how test organizations carry out the software test activities.

As part of the OT Evaluation Framework, the TEMP should 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:

- 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, and 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

- Carnegie Mellon Software Engineering Institute, Draft Special Report CMU/SEI-2018-SR-013. *DoD Developer's Guidebook for Software Assurance* (February 2018)
- Joint Software Systems Safety Engineering Handbook, Developed by Joint Software Systems Safety Engineering Workgroup (2010).
- US DoD, MIL-STD-882E, Department of Defense Standard Practice System Safety (2012).
- NASA-GB-8719.13, Software Safety Guidebook. NASA-GB-8719.13. Developed by: National Aeronautics and Space Administration (2004).
- NASA-STD-8739.9, Software Formal Inspection standard. Developed by: National Aeronautics and Space Administration (NASA) (2013).
- State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation. Developed for Office of the Deputy Assistant Secretary of Defense for Systems Engineering; by the Institute for Defense Analyses. (2016)
- Trusted Systems and Networks (TSN) Analysis, Developed by DASD (SE) and DoD CIO (June 2014).

Appendix X1 Considerations for Cybersecurity Requirements and Measures for DT&E (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/resp/CTT>

Appendix X2 Cyber Threat Assessment for Cybersecurity T&E (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/resp/CTT>

Appendix X3 Mission-Based Cybersecurity Risk Assessments (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/resp/CTT>

Appendix X4 Cybersecurity Test Infrastructure and Environment Planning (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/resp/CTT>

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/resp/CTT>