Department of War
Cyber Developmental Test and Evaluation Guidebook

Version 3.1

March 5, 2026

Office of the Under Secretary of War for Research and Engineering

Office of the Assistant Secretary of War for Mission Capabilities

Washington, D.C.

Distribution Statement A. Approved for public release. Distribution is unlimited.

The appearance of external hyperlinks does not constitute endorsement by the United States Department of War (DoW) of the linked websites, or the information, products, or services contained therein. DoW does not exercise any editorial, security, or other control over the information you may find at these locations.

Department of War Cyber Developmental Test and Evaluation Guidebook

Office of the Under Secretary of War for Research and Engineering
Office of the Assistant Secretary of War for Mission Capabilities
Office of the Deputy Assistant Secretary of War for Multi-Domain Joint Operations
Developmental Test, Evaluation, and Assessments
3030 Defense Pentagon
Washington, DC 20301-3030
osd.r-e.comm@mail.mil
https://www.cto.mil/dtea/cyber

Distribution Statement A. Approved for public release. Distribution is unlimited.
DOPSR Case # 25-T-1827.

Approved by
Mr. Thomas W. Simms
Principal Deputy, Multi-Domain Joint Operations

Thomas Simms Digitally signed by Thomas Simms
Date: 2026.10.08 13:07:08 -04'00'

DoW Cyber DT&E Guidebook Change Record

Date	Change/Version	Summary of Changes
1 July 2015	Version 1.0	Initial release, version 1.0
25 April 2018	Version 2.0	Initial release, version 2.0
4 November 2019	Version 2.0, Change 1	Updated chapters 2–11, Appendices A, C, and G.
27 June 2025	Version 3.0	Alignment with the forthcoming DoD Manual 5000.UY; focuses solely on cyber DT&E and supersedes phases 1–4 in previous versions.
5 March 2026	Version 3.1	Updated DoD Manual 5000.UY to DoW Manual 5000.103, Department of Defense updated to Department of War (where able), and other minor edits.

Executive Summary

This guidebook provides technical information and critical best practices for ensuring Department of War (DoW) systems are survivable and operationally resilient in contested or hostile cyber environments. Aligned with DoW Manual 5000.103, "Cyber Developmental Test and Evaluation," it offers practical "how-to" guidance for planning, preparing, executing, evaluating, and reporting cyber developmental test and evaluation (DT&E) activities across the system life cycle from concept development through sustainment.

Version 3.0 significantly enhanced cyber DT&E by fully supporting the Adaptive Acquisition Framework (AAF), non-acquisition, and pre-acquisition systems. With Version 3.1, the department name has been updated to Department of War where those changes are able to be made. In some cases, the use of "Department of Defense" or "DoD" cannot be updated yet. References to the "forthcoming DoD Manual 5000.UY" have been updated to DoW Manual 5000.103.

The guidebook is not restrictive or all encompassing. Instead, the guidebook enables consistent application of the practices throughout DoW for every technology or system supporting warfighting missions while encouraging analysis and tailoring to support responsive testing strategies. The former six-phase approach is replaced, offering greater flexibility for organizations to adapt processes to their unique requirements and pursue rigorous test-fix-test system developer cyber DT&E.

This guidebook is intended for technical practitioners involved in cyber DT&E and provides the best currently available guidance. Organizations should leverage these practices while adapting them to their specific needs and schedules.

These updates collectively aim to improve the effectiveness and adaptability of cyber DT&E within DoW, ensuring that robust and modern test and evaluation (T&E) practices can meet the pace and agility of evolving technology development and acquisition strategies.

Future versions will integrate cyber DT&E and operational T&E guidance, further strengthening DoW's T&E capabilities.

Mr. Thomas W. Simms
Principal Deputy, Multi-Domain Joint Operations

Contents

1 Introduction 1
1.1 Organization of this Guidebook 1
1.2 Audience, Purpose, and Usage 3
1.3 Applicability 4
1.4 Terminology 5
1.5 Cyber Policies and Guidance for Acquisition Programs and Systems 7
1.5.1 DoW Manual 5000.103 7
1.5.2 Policies Relevant to Cyber DT&E 7
1.6 Integrating Cyber Testing 10
1.6.1 Integrating System Developer and Government Testing 11
1.6.2 Integrating Government Cyber Developmental and Operational Testing 11
1.7 Concurrent Cyber and Non-Cyber Testing 12
1.8 Summary of Integrated and Concurrent Cyber Testing 13
2 Cyber DT&E Overview 14
2.1 Iterative Planning, Preparing, Executing, Evaluating, and Reporting 14
2.1.1 Iterative and Recursive Nature 15
2.1.2 Tailoring Cyber DT&E for S&T, Pre-Acquisition, AAF, or Service-Internal Approaches 16
2.2 Cyber Working Group 17
2.2.1 CyWG Formation and Authorities 17
2.2.2 Recommended CyWG Participants and Roles 19
2.2.3 Documentation, System-Relevant Artifacts, and Data Management to Support Cyber DT&E 19
2.3 Early CyWG, Test Team, and Analyst Involvement 21
2.4 Role of Scientific Test and Analysis Techniques in Cyber DT&E 21
2.5 Cyber DT&E Relationship to System Security Engineering 23
3 Iterative Planning for Cyber DT&E 25
3.1 Cadence 25
3.2 Inputs 26
3.3 Activity: Cyber DT&E Strategy Scoping 27
3.3.1 Task: Examine and Advise on Cyber Requirements 28
3.3.2 Task: Examine Current Threat Assessments 32
3.3.3 Task: Characterize the Attack Surface 33
3.3.4 Task: Support Criticality Analysis 34
3.3.5 Task: Conduct Mission Based Cyber Risk Assessments 35
3.3.6 Task: Use Prior Test Results 36

3.4 Activity: CyWG Input to System Developer Contract Requirements 36
3.5 Activity: Cyber DT&E Iterative Input to the TEMP or T&E Strategy 36
3.5.1 Task: Synchronize Content with the Cybersecurity Strategy 38
3.5.2 Task: Refine and Update the Cyber DT&E Strategy 39
3.6 Artifact Generation 40

4 Preparing for Cyber DT&E 41
4.1 Inputs 41
4.2 Activity: Gather Detailed Cyber DT&E Plan Information 43
4.2.1 Task: Determine Contractual Basis and Pre-Work 46
4.2.2 Task: Define the Test Type(s) 46
4.2.3 Task: Develop Cyber DT&E Test Objectives 49
4.2.4 Task: Understand Commercial Infrastructure Interfaces 52
4.2.5 Task: Document Unique Considerations for Specialized Assets and Techniques 53
4.3 Activity: Develop the Test Plan 57
4.4 Activity: Prepare for Cyber DT&E Events 61
4.5 Activity: Conduct Cyber DT&E Readiness Reviews 63
4.6 Artifact Generation 65

5 Executing Cyber DT&E 66
5.1 Inputs 66
5.2 Activity: Conduct the Test 66
5.2.1 Task: Perform Setup, Validation, and Checkout 67
5.2.2 Task: Perform Baseline and Risk-Reduction Test and Evaluation 67
5.2.3 Task: Conduct Test for Score and Capture Test Result Data 68
5.2.4 Task: Determine Test Closeout 70
5.3 Artifact Generation 70

6 Evaluating Cyber Developmental Test Data 72
6.1 Inputs 72
6.2 Activity: Cyber Developmental Test Evaluation 72
6.2.1 Task: Organize the Data 72
6.2.2 Task: Review Data and Define Evaluation Focus 72
6.2.3 Task: Synthesize and Correlate Findings 73
6.2.4 Task: Analyze Performance and Risk 73
6.2.5 Task: Prepare Conclusions 74
6.3 Artifact Generation 74

7 Reporting Cyber DT&E Results 77

7.1 Inputs 78
7.2 Activity: Develop Cyber DT&E Reports 78
7.3 Artifact Generation 80
7.4 Evidence/Data Management 81

8 Cyber DT&E Process Challenges and Digital Engineering Considerations 83
8.1 Non-Acquisition and Pre-Acquisition 84
8.2 Adaptive Acquisition Framework Pathway Considerations 85
8.3 Considerations for Systems, Subsystems, Components, and Subcomponents of Uncertain Pedigree 85
8.4 Strategies for Tackling Cyber DT&E Process Challenges 86
8.5 Model-Based Systems Engineering and Digital Engineering 94
8.5.1 Digital Twins in Cyber DT&E 95
8.5.2 Modeling and Simulation in Cyber DT&E 97
8.5.3 Cyber Analytic Tools Support CyWG Activities 98
8.5.4 Leveraging Ontologies for Enhanced Cyber DT&E in MBSE and DE 99

Appendix A: Considerations for Staffing Cyber DT&E Activities 102

Appendix B: Examine and Advise on Cyber Performance Requirements and Measures for Cyber DT&E 123

Appendix C: Key System Artifacts for Cyber DT&E Analysis and Planning 139

Appendix D: Cyber Threat Assessment for Cyber DT&E 153

Appendix E: Attack Surface Characterization 164

Appendix F: ICT Supply Chain Cyber DT&E Considerations 174

Appendix G: Mission Based Cyber Risk Assessments 192

Appendix H: Cyber DT&E of DoW Systems Using Commercial Cloud 218

Appendix I: Incorporating Cyber DT&E into DoW Contracts 242

Appendix J: Cyber DT Infrastructure and Environment Planning 267

Appendix K: Cyber DT&E Strategy Considerations 274

Glossary 284

Acronyms 285

References 293

Figures

Figure 1-1. DoW RMF Symbol 7
Figure 1-2. Combining Cyber Testing: Integrated and Concurrent 13
Figure 2-1. Cyber DT&E Iterative Process 14
Figure 2-2. Cyber DT&E Process Is Iterative and Recursive 15
Figure 2-3. Notional CyWG Charter Outline 18
Figure 2-4. CyWG Representatives and Responsibilities 19
Figure 2-5. STAT Process 22
Figure 4-1. JETEP Website 63
Figure 5-1. Example Data Collection Form 69
Figure 8-1. Cyber DT&E Activities – A Campaign of Learning to Support Decisions 85
Figure 8-2. The OACRA Viewer Systems View 101
Figure A-1. WU Cyber T&E Foundational Credential Pathway, Under Development 102
Figure A-2. Proposed WU Courses for the System Testing and Evaluation Specialist DCWF Role 103
Figure A-3. Vulnerability Analyst Proficiency and Maturity Levels 110
Figure A-4. Example RACI Matrix 119
Figure A-5. JETEP Homepage 122
Figure B-1. HAT TRICK Cyberspace Threat Event Matrix 125
Figure B-2. High-Level Notional Overview of the Cyber Test Metric Derivation Process 130
Figure B-3. Ishikawa Diagram for Reducing Software Risk 132
Figure B-4. Verification and Validation Occurs Throughout the Life Cycle 135
Figure D-1. Notional Intelligence Support Request Form 155
Figure D-2. Intelligence Unit and IPC Cyber Threat Production Flowchart 158
Figure D-3. Example Risk-Level Matrices 162
Figure D-4. Example Intelligence Language to Risk Language Conversion Flowchart 162
Figure E-1. Wheel of Access 165
Figure G-1. MBCRA Critical Elements 193
Figure H-1. Cloud Service Models 219
Figure H-2. Notional DoW Cyber DT&E Scope by Cloud Service Model Type 220
Figure H-3. Cloud Integration with the DoDIN Architecture 227
Figure H-4. Examples of Key Architectural and Operational Elements 230
Figure K-1. IDSK for Better Decisions and Warfighter Capabilities 279

Figure K-2. IDSK Static Construct of Framework Elements 280
Figure K-3. Notional Cyber Survivability Section of an IDSK 281

Tables

Table 1-1. Guidebook Sections and Appendices 1
Table 1-2. Policies and Guidance Relevant to Cyber DT&E 8
Table 4-1. Cyber DT&E Activities, Facilities, Assets, and Types 48
Table 4-2. Example Test Objectives 50
Table 4-3. Example Test Plan Outline 58
Table 6-1. Evaluate Data Collection 74
Table 7-1. Vulnerability Class 80
Table 7-2. Cyber DT&E Assessment Considerations for Stakeholder Reporting 80
Table A-1. CyWG Participant Roles 115
Table A-2. Organizational Cyber DT&E Standards 120
Table B-1. High-Level HAT TRICK Requirements Examples 125
Table B-2. Characteristics of Good Test Metrics 135
Table C-1. Artifacts Supporting Test Planning Guidance 139
Table C-2. Potential Sources to Inform Iterative Planning for Cyber DT&E 144
Table D-1. Key Intelligence Support Actions 154
Table D-2. Supporting Documentation Inputs 156
Table D-3. Typical Production Request Form Contents 157
Table D-4. Intelligence Reporting Threat Tiers 160
Table D-5. Intelligence Reporting Likelihood Ratings 160
Table D-6. Intelligence Reporting IC Confidence Levels 161
Table F-1. Examples of SBOM Attribute Analysis 180
Table G-1. Input Element 193
Table G-2. Prepare Element 196
Table G-3. Planning Activities 196
Table G-4. Methodology Selection Considerations 198
Table G-5. Execute Element 203
Table G-6. Output Element 205
Table G-7. MBCRA Attribute Inputs to Documentation 210
Table G-8. MBCRA–DoW RMF Correlation 213

Table G-9. Common MBCRA Questions and Answers 214
Table H-1. Cloud Information Impact Levels..... 222
Table H-2. FedRAMP Artifacts for Use by Cyber DT&E 232
Table H-3. Cloud Cyber Test Objectives Aligned to Current Cloud Security Threats 238
Table I-1. Test-Related NIST RMF Controls 245
Table I-2. Test-Related Contract Deliverables 264
Table J-1. Cyber DT&E Test Infrastructure Planning Considerations 268
Table K-1. Program Protection Requirements..... 276
Table K-2. Cyber DT&E in Test and Evaluation Management..... 277
Table K-3. Resources for Cyber Developmental Tests 282

1 Introduction

This guidebook complements the Department of War (DoW) Manual (DoWM) 5000.103, "Cyber Developmental Test and Evaluation." DoWM 5000.103 provides "what" to do, whereas this guidebook outlines "how to" implement guidance, offering practical approaches for those tasked with executing cyber developmental test and evaluation (DT&E). Cyber DT&E is a continuum of test and evaluation (T&E), conducted iteratively as changes in the system occur and as threat scenarios evolve. Cyber DT&E is not a one-time activity providing static information but is iterative throughout development to update and expand the evidence base, delivering data for decisions as part of a campaign of learning. The frequency of T&E activities and their cadence depends on the defined purpose and scope of assessments needed during development.

The guidebook offers direction and guidance without restricting the solution space available to DT&E practitioners. Deviations should be intentional and justifiable. Organizations are accountable for ensuring that their chosen methods, structures, and activities align to their situation and to the system's mission context.

This guidebook highlights the boundaries and integration points between related disciplines, including program protection, systems engineering (SE), system security engineering (SSE), risk management, operational test and evaluation (OT&E), and software assurance. Although this is not an all-inclusive list, each of these disciplines intersect with cyber DT&E. Practitioners should manage those intersections through coordination and teamwork.

1.1 Organization of this Guidebook

This guidebook has eight sections and 13 appendices, as outlined in Table 1-1, and includes a glossary, acronym list and a list of references. Each section provides a solid and workable basis of knowledge. The appendices are topic-specific, detailed treatments of a particular focus area to provide in-depth and specific guidance, including not only "how" but "why."

Table 1-1. Guidebook Sections and Appendices

Section/Appendix	Content Description	Key Takeaways/Process Documented
Sections 1 and 2	Foundational information and processes	Introduces the concepts, terminology, and methodologies applied throughout the guidebook
Sections 3–7	Iterative cyber DT&E process	Comprehensive documentation of the process for iterative planning, preparing, executing, evaluating, and reporting a cyber DT&E campaign

Section/Appendix	Content Description	Key Takeaways/Process Documented
Section 8	Cyber DT&E process challenges and digital engineering considerations	Provides insights and considerations on risks affecting cyber DT&E processes and applying guidance to non-acquisition, pre-acquisition, and acquisition programs using the Adaptive Acquisition Framework pathways
Appendix A:	Considerations for staffing cyber DT&E activities	Provides considerations when staffing cyber DT&E activities
Appendix B:	How to examine and advise on cyber performance requirements and measures for cyber DT&E	Provides guidance for understanding performance requirements and measures for cyber DT&E
Appendix C:	Key system artifacts for cyber DT&E analysis and planning	Provides a compilation of essential system artifacts instrumental for T&E leads, the cyber working group, and the cyber test team to analyze and apply during cyber DT&E
Appendix D:	Cyber threat assessment for cyber DT&E	Describes methods for obtaining cyber threat assessments
Appendix E:	Attack surface characterization	Focuses on considerations for evolving attack surfaces
Appendix F:	Information and communications technology supply chain cyber DT&E considerations	Emphasizes the integration of cybersecurity considerations into all stages of the information and communications technology supply chain
Appendix G:	Mission based cyber risk assessments	Explains how to conduct mission based cyber risk assessments
Appendix H:	Cyber DT&E of DoW systems using commercial cloud	Discusses the implications and considerations for conducting cyber DT&E of DoW systems using commercial cloud platforms
Appendix I:	Incorporating cyber DT&E into DoW contracts	Highlights the essential considerations for cyber DT&E in contracts
Appendix J:	Cyber developmental test infrastructure and environment planning	Provides guidance on planning for adequate test infrastructure and environments
Appendix K:	Cyber DT&E strategy considerations	Outlines the essential content for a cyber DT&E strategy
Controlled Unclassified Information (CUI) Appendix L	Cyber DT&E of specialized assets	Available using a CAC at Appendix L (CAC)
Digital Appendix M	Cyber DT&E for artificial intelligence-enabled systems	Available at Appendix M

1.2 Audience, Purpose, and Usage

The guidebook's intended audience comprises the diverse stakeholders represented in the cyber working group (CyWG), including:

- T&E practitioners.
- DT&E stakeholders with cyber DT&E execution responsibility.
- Science and technology (S&T) and pre-acquisition managers.
- System developer managers.
- Program managers and those with decision authority for activities enabling cyber T&E.

Refer to Section 2.2 for more information on the CyWG formation and participants. Additionally, the guidebook considers the roles of:

- Senior decision makers.
- Program executives.
- Oversight organizations.
- Authorizing officials (AOs).
- Functional, requirements, and solution sponsors.
- Transitioning technology program and S&T managers.
- Warfighters.
- System development and DT&E test teams.
- Operational test agencies (OTAs).
- Operational test organizations (OTOs).
- Industry partners in the execution of cyber DT&E.

This guidebook promotes data-driven and mission-impact-based analysis and assessment methods for cyber DT&E. It supports the assessment of system cybersecurity and cyber resilience within a mission context by encouraging planning for tighter integration with traditional system T&E. Cyber DT&E starts as early as possible and continues throughout the entire life cycle. Cyber DT&E iteratively and recursively verifies the development of cyber survivable and operationally resilient systems through evaluation of the system's cybersecurity and cyber resilience performance requirements in support of assigned missions.

This guidebook assumes that the user has a working knowledge of DoW implementation of the Risk Management Framework (RMF). Cyber DT&E is iterative, starts as early as possible, and should integrate as many data sources as available. This guidebook recognizes that cyber DT&E and DoW RMF processes may be complementary; however, cyber DT&E exists outside of the requirement for the DoW RMF, and the concepts in the guidebook are not dependent on the DoW RMF. The DoW RMF is a necessary process to support gaining and updating an authorization to operate (ATO), but it does not replace cyber DT&E. Assessment and authorization processes should inform DT&E but are not substitutes for DT&E.

1.3 Applicability

This guidebook applies to all DoW systems, including non-acquisition prototyping and development; pre-acquisition program technologies and systems; acquisition systems in accordance with Department of Defense (DoD) Directive (DoDD) 5205.07, "Special Access Program Policy"; systems acquired via the War Acquisition System; and systems in sustainment. These systems include:

- Acquisition programs:
  - Urgent capability acquisition (UCA).
  - Middle tier of acquisition (MTA).
  - Major capability acquisition (MCA).
  - Software acquisition.
  - Defense business systems (DBS).
  - Acquisition of services.
- Hull, mechanical, and electrical systems.
- Industrial control systems.
- National security systems (NSS).
- Non-developmental items (NDIs).
- Supervisory control and data acquisition systems.
- Weapon systems.

How Much Cyber DT&E is Enough?

Multiple factors govern the depth and extent required for cyber DT&E. The primary considerations are the system's longevity and the mission or safety criticality of the computational elements. These considerations drive the level of rigor in developing and sustaining the cyber resilience posture for the computational elements of the system. Parallel rigor and thoroughness of iterative cyber DT&E are required to verify cybersecurity effectiveness and cyber resilience performance.

This guidebook applies to any cyber DT&E including testing across the interfaces between and on the digital subcomponents of a larger system or service (e.g., cloud service); components of a system or service; subsystems; systems; systems of systems (SoS); platforms or families of systems; and any digital technology for use by DoW. Cyber DT&E informs decision makers

about the existence and importance of technical vulnerabilities measurably affecting functional mission execution and operational resilience.

1.4 Terminology

Cyber DT&E uses people, tools, data, and artifacts to perform the activities related to quantifying and characterizing a system's cyber survivability and operational resilience capabilities within a mission context.

Cyber DT&E as Defined in DoWM 5000.103

The subset of T&E activities, tools, data, and artifacts used to create independently verifiable and substantiated knowledge to quantify and characterize the cyber resilience of a system, subsystem, component, and software or to create independently verifiable and substantiated information to quantify and characterize cyber-related utility and risks of new technologies under development (e.g.,

The Military Services/DoW Components/ Agencies and other organizations involved in cyber DT&E may use different terms for the people or teams discussed in this guidebook. Accomplishing the actions and activities described in this document is more important than conforming with the titles of those performing the activities. DoWM 5000.103's glossary and the Glossary in this guidebook define the terms commonly used in this document. Appendix A: discusses the key personnel involved in the iterative planning, preparing, executing, evaluating, and reporting of cyber DT&E.

Two terms used throughout this guidebook when discussing cyber DT&E activities are "stakeholders" and "cyber DT&E teams."

The term "stakeholders" refers to the organizations and personnel consulted, informed, or accountable for decisions involving cyber DT&E, including:

- Office of the Secretary of War (OSW) oversight organizations, for example, the Under Secretary of War for Research and Engineering; the Director, Developmental Test, Evaluation, and Assessments; and the Director, Operational Test and Evaluation.
- Military Services/DoW Components/Agencies decision authorities (DAs).
- Functional, requirement, or solution sponsors.
- Combatant Commands, mission owners, warfighters.
- Acquisition program management offices.
- Acquisition program managers.
- S&T managers.

- Chief developmental testers (CDTs) or T&E leads.
- Lead DT&E organizations (LDTOs).
- Cyber DT&E organizations.
  - Participating test organization.
  - Executing test organization.
- OTAs/OTOs.
- AOs.

The term "cyber DT&E teams" or "test teams" refers specifically to the test organizations and personnel responsible for conducting cyber DT&E and can include representatives from this list:

- Industry and government contractors or system developers.
- Government test organizations.
- DoW cyber assessment teams (DCATs).
- DoW Cyber Red Teams (DCRTs).
- Data collectors.
- Evaluators.

The guidebook uses a single phrase to represent many interpretations of a word, term, or phrase, including:

- **System developer**: The contractor, vendor, service provider, original equipment manufacturer, software developer, or any organization delivering the subcomponent, component, subsystem, system, service, SoS, family of systems, or platform of systems. The system developer may be a government-run organization with or without contractors performing the service or system development or may be an industry contractor, a small business contractor, or a major prime contractor.
- **System under test (SUT)**: The acronym "SUT" refers to the "system under test" for a particular cyber DT&E event or activity. The SUT is the focus for a test plan and test report. A SUT may refer to a subcomponent of a larger system or service (e.g., cloud service), component of a system or service, subsystem, system, SoS, platform or family of systems, relevant interfaces between them, and any digital technology depending on the context of the cyber DT&E event. The SUT may also include nonmaterial systems such as a depot or local maintenance process or software assurance process.

- **Program manager**: This guidebook uses the term "program manager" to refer to the decision maker responsible for managing the cost, schedule, and performance—for example, acquisition program managers, S&T managers, project leads, or the equivalent—for non-acquisition prototyping and development, pre-acquisition program technologies and systems, program of record (POR) acquisition systems, systems acquired via the War Acquisition System, or systems in sustainment.
- **Program manager's organization**: This guidebook uses the phrase "program manager's organization" to encompass any office or organization leading the non-acquisition, pre-acquisition, or acquisition effort.
- **DoW RMF**: This guidebook uses the DoW RMF symbol depicted in Figure 1-1 to highlight DoW RMF and cyber DT&E alignment.



Figure 1-1. DoW RMF Symbol

1.5 Cyber Policies and Guidance for Acquisition Programs and Systems

The following subsections briefly discuss cyber policies relevant to cyber DT&E, but the list is not exhaustive. Reminder: This guidebook contains generalized content.

1.5.1 DoW Manual 5000.103

DoWM 5000.103 emphasizes initiating testing early and iteratively throughout the system's life cycle and ensuring mission-focused cyber DT&E. DoWM 5000.103 applies to all DoW systems and services, including non-acquisition and pre-acquisition technologies and systems, acquisition systems, systems acquired via the War Acquisition System, systems in sustainment, or post-production systems based on specified changes in the system, mission, threat, or other factors. DoWM 5000.103 prescribes the procedures and processes for DoW Components to plan, fund, execute, and report on cyber DT&E. Cyber DT&E procedures provide engineers and decision makers with information to measure progress, identify problems, characterize system capabilities and limitations, and manage technical and programmatic risks.

1.5.2 Policies Relevant to Cyber DT&E

Table 1-2 briefly describes some policies and guidance most relevant to the cyber DT&E activities in this guidebook. For additional details on Adaptive Acquisition Framework (AAF) policies, go to the Warfighting Acquisition University (WU) AAF Website at https://aaf.dau.edu.

Refer to the most recently published version of each DoW issuance available on the DoW Issuances Website (https://www.esd.whs.mil/DD/DoD-Issuances/).

Table 1-2. Policies and Guidance Relevant to Cyber DT&E

AAF Functional or Other Relevant Policy	Purpose and Cyber T&E Relevance
DoDD 5200.47E, "Anti-Tamper (AT)"	Requires DoW Components to determine requirements for, plan, design, implement, test, and evaluate AT based on the consequence of CPI compromise and the anticipated system exposure in accordance with DoDI 5200.39 and in alignment with requirements guidance from the DoW Executive Agent for AT.
DoDI 5000.82, "Requirements for the Acquisition of Digital Capabilities"	• Establishes functional acquisition policy and procedures for all acquisition programs containing information technology (IT) (including national security systems (NSS)), including modular open systems approaches and integration with other systems engineering (SE) and system security engineering for the program. • Requires that the acquisition of systems containing IT, including NSS, include the planning and execution of an efficient and effective T&E program. • Requires all systems containing IT to develop a cybersecurity strategy.
DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage"	• Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; information and communications technology supply chain exploitation; and reverse engineering. • Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans, S&T protection, Program Protection Plans, and engineering cybersecurity activities.
DoDI 5000.86, "Acquisition Intelligence"	• Establishes policy, assigns responsibilities, and provides direction for the integration of intelligence in the acquisition life cycle. • Requires integration of threat representations into the Test and Evaluation Master Plan. Specifies the threat focus to be initial operational capability plus 10 years but does not specifically address cyberspace threats. Specifying the cybersecurity threat for the future is a challenge because of the dynamic nature of cybersecurity. Design should focus on what is controllable by the acquisition program office.

AAF Functional or Other Relevant Policy	Purpose and Cyber T&E Relevance
	• Requires acquisition planners to document how intelligence requirements will be integrated into T&E activities.
DoDI 5000.88, "Engineering of Defense Systems"	Requires a concept design review before the materiel development decision and notes that the concept baseline should include a cybersecurity assessment.
DoDI 5000.89, "Test and Evaluation"	• Establishes policy for DT&E across five of the six acquisition pathways. • Requires cyber DT&E and the use of this guidebook. • Requires that acquisition programs perform mission based cyber risk assessments.
DoDI 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers"	Establishes policy for acquisition program managers and decision authorities to manage their cybersecurity risk in the DoW acquisition processes.
DoDI 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)"	• Requires the identification and protection of critical program information (CPI), including the testing of those protections. • States that protections include anti-tamper (AT) and cybersecurity measures (among others). • Includes defense exportability features as a potential protection measure for CPI.
DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks"	Implements the trusted systems and networks strategy, which integrates cybersecurity into the SE process.
DoDI 8500.01, "Cybersecurity"	• Defines and requires DT&E for operational resilience, risk management, integration, and interoperability. • Incorporates cybersecurity considerations early and continuously within the acquisition life cycle. • Requires cyber T&E throughout the acquisition life cycle. • Plans, resources, and integrates cybersecurity assessments into DT&E and as part of T&E assessments. • Integrates cyber T&E with interoperability and other functional testing; a cybersecurity representative participates in the planning, execution, and reporting of integrated test activities.
DoDI 8510.01, "Risk Management Framework for DoD Systems"	• Integrates DoW RMF activities with developmental and operational test activities. • Defines specific concepts and rules for testing to support reciprocity between acquisition program offices to reduce redundant testing, assessments, documentation, and the associated costs in time and resources.

AAF Functional or Other Relevant Policy	Purpose and Cyber T&E Relevance
DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations"	• Supports DoW RMF requirements to monitor security controls continuously. • Requires the testing of defensive cyberspace operations.
Manual for the Operation of the Joint Capabilities Integration and Development System Joint Staff publications are available at: https://www.jcs.mil/Library/	• Encourages requirements developers to leverage the Cyber Survivability Endorsement Implementation Guide regarding the System Survivability (SS) Key Performance Parameter (KPP). • Resource managers, functional sponsors, and others define up to 10 cyber survivability attributes as part of the SS KPP in requirements documents.

1.6 Integrating Cyber Testing

Integrating cyber testing (including system developer and government testing) allows sharing a test point, event, or evaluation result to support multiple independent objectives without compromising the test objectives of either the system developer or government test team or of the government test organizations. Integrating testing does not replace or eliminate the need for a dedicated cyber DT&E effort but can reduce the overall amount of cyber testing required. Integrating test events supports comprehensive evaluation of system subcomponents through fully integrated systems as early as possible and may enable accelerated delivery timelines. The CyWG should consider planning for any of the approaches described below.

For any integrated test efforts, the CyWG documents the components of integrated cyber tests in the T&E strategy. The CyWG should always plan cyber DT&E to integrate with and support DoW RMF assessment requirements.

The CyWG should form an integrated cyber test team composed of the relevant stakeholders. The integrated cyber test team reviews CyWG priorities for testing and creates test objectives and test plans for approval by the appropriate authorities as early in system development as possible. The integrated cyber test team should use the Integrated Decision Support Key (IDSK), documented in the Test and Evaluation Master Plan (TEMP) or other T&E strategy, to identify opportunities for tests, updating the Integrated Master Schedule or equivalent, the IDSK, and the TEMP or T&E strategy to reflect the changes. For more information on the IDSK, see Section K.2.7. Early planning enables identifying the test resources needed to support the integrated events.

As the CyWG seeks opportunities for integrated cyber testing, they should consider answering the following questions:

- Do system maturity and test conditions meet stakeholder requirements?

- Do opportunities exist where a test provides the conditions necessary for an integrated approach?
- Have stakeholders reviewed all proposed test events to determine the feasibility of shared data to meet their needs?
- Do agreements on data management and sharing exist to enable the sharing of data?
- Do all affected stakeholders agree that an event proposed for integrating cyber testing will provide information to meet their needs?
- Do available artifacts, such as the request for proposal (RFP), statement of work (SOW), or statement of objectives (SOO) need language to enable integrated cyber test approaches?

1.6.1 Integrating System Developer and Government Testing

The CyWG assists with the creation of contract language enabling integrated system developer–government cyber test activities (including the use of system developer test facilities and mission based cyber risk assessments (MBCRAs)) and government data rights to developer test data (including component testing data, commercial cloud data, and access to appropriate databases). The CyWG should provide input for the RFP, SOW, or SOO. See Appendix I: for additional contract language recommendations.

CyWG Involvement in Contract Language

Early CyWG involvement in developing the contract language is critical to cyber DT&E. Involvement in the contract is the first component of planning the event.

See Sections 2.2 and 2.3 for more information on CyWG roles and early test involvement.

See Appendix I: for suggested contract considerations.

1.6.2 Integrating Government Cyber Developmental and Operational Testing

The CyWG identifies opportunities for integrated cyber test events to satisfy DT&E and OT&E test objectives. Integrating DT&E with OT&E can enable fewer overall testing events and deliver earlier insights into system performance and effectiveness. Joint interoperability test events may provide opportunities to integrate cyber testing.

Key considerations for planning integrated government cyber tests include:

- **SUT developmental and design maturity**. This consideration requires operators (as opposed to system developers) to use a SUT that is sufficiently production representative in a mission-relevant environment.

- **Conditions of test**. The CyWG should understand if the test planners will create representative operational conditions for measures and data of interest. For example, the CyWG should confirm that the test includes connections to external networks and systems to expose the SUT to expected external and internal network traffic types and volumes. They should confirm whether the SUT requires an ATO or authorization to connect (ATC) before testing if the SUT is connected to external networks.
- **T&E strategy**. The cyber T&E strategy in an approved TEMP or T&E strategy should provide guidance to establish expectations on the composition and specific timing of integrated cyber tests.
- **Verification, validation, and accreditation (VV&A) status**. When using a developmental environment to satisfy testing requirements, the OTA/OTO will need to verify that the emulated environment is sufficiently realistic and has completed required VV&A.
- **Team knowledge and experience**. Cyber DT&E test teams often have in-depth system and mission knowledge and experience with system-specific vulnerabilities. Cyber OT&E test teams typically have a broad perspective of common vulnerabilities and tactics, techniques, and procedures (TTPs) across systems but often lack system- and mission-specific knowledge. Having DT&E and OT&E representation for test planning and during the other's tests creates synergy and prevents teams from spending unnecessary time on previously covered ground or unfruitful exploitation attempts. Each team also learns valuable skills and information from working with the other team, making them more effective in their respective roles.

1.7 Concurrent Cyber and Non-Cyber Testing

The CyWG should plan some cyber test events to occur concurrently with other test events, including the testing of functional performance, interoperability, and other nonfunctional operational and support requirements (e.g., reliability, availability, maintainability, supportability). Early functional performance, lab-based, bench, or model-based engineering tests and simulations performed during system development demonstrate technology maturity toward meeting threshold requirements; provide an early perspective on components; and verify and validate capabilities and limitations. Conducting cyber DT&E during functional DT&E may provide opportunities to test the same requirements in the presence of cyber effects to inform the assessment of operational resilience and cyber survivability.

Identifying the SUT's ability to execute functions in support of defined missions in contested cyber conditions can inform early design modifications to improve mission functional performance and cyber defensibility.

The CyWG should assist with contract language to have the system developer perform concurrent cyber and non-cyber testing with government representatives observing the tests. The CyWG should also assist with contract language to provide the test articles and digital models that may facilitate government-performed concurrent cyber and non-cyber testing.

Example: Restoration Requirement

System restoration required within a specific mission timeline, including detection, logging, etc.

If feasible, test teams should conduct SUT recovery and restoration testing during concurrent cyber and non-cyber testing. The testing enables assessing whether the SUT can recover mission capability in time to allow critical mission operations to continue uninterrupted after experiencing effects from an attack and enables assessing any responses to the attack based on the threat profile.

1.8 Summary of Integrated and Concurrent Cyber Testing

Figure 1-2 briefly describes integrated and concurrent cyber testing and provides suggested timelines.

"Integrated testing requires the collaborative planning and execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders."

– DoDI 5000.89

Test Type	Timeline	Description
Integrated Contractor and Government Testing	During engineering, development	Complete a comprehensive evaluation of cyber performance for critical system sub-components through fully integrated systems as early as possible in the acquisition pathway
Concurrent Cyber and non-Cyber Testing	During engineering, development, early government DT	Early lab-based, bench, or model-based engineering tests performed during system development to demonstrate meeting the following types of threshold requirements in contested cyber environments: • Key performance parameters (KPPs) • Key system attributes (KSAs) • Other performance and mission related measures unique to the program
Integrated Government Cyber DT-OT	After delivery to the government	Measure mission effects and the system/operator response in cyberspace Independent evaluations of common use data collection

Independent assessment/evaluation of data

Figure 1-2. Combining Cyber Testing: Integrated and Concurrent

2 Cyber DT&E Overview

2.1 Iterative Planning, Preparing, Executing, Evaluating, and Reporting

The cyber DT&E continuum uses planning activities and tasks, system developmental trigger points (based on system maturity and updates), and a choice of tactics (cooperative, adversarial, both) and tests supportive of test objectives to provide practitioners with more flexibility in individual event construction. This iterative and recursive testing strategy means a system is not necessarily "test complete" at the completion of an adversarial assessment or when fielded. Cyber DT&E should start as early as possible in the life cycle (e.g., concept development, requirements development) and follow a test-fix-test approach using the planning activities and tasks to inform the *Preparing* activities and tasks per test event. The CyWG should be mindful to allocate sufficient time during "fix" to ensure that remedies occur before moving to subsequent steps. Cyber DT&E test events do not have specific duration requirements.

Figure 2-1 is an enhanced visual of the cyber DT&E process depicted in and implemented in accordance with Section 4 of DoWM 5000.103.

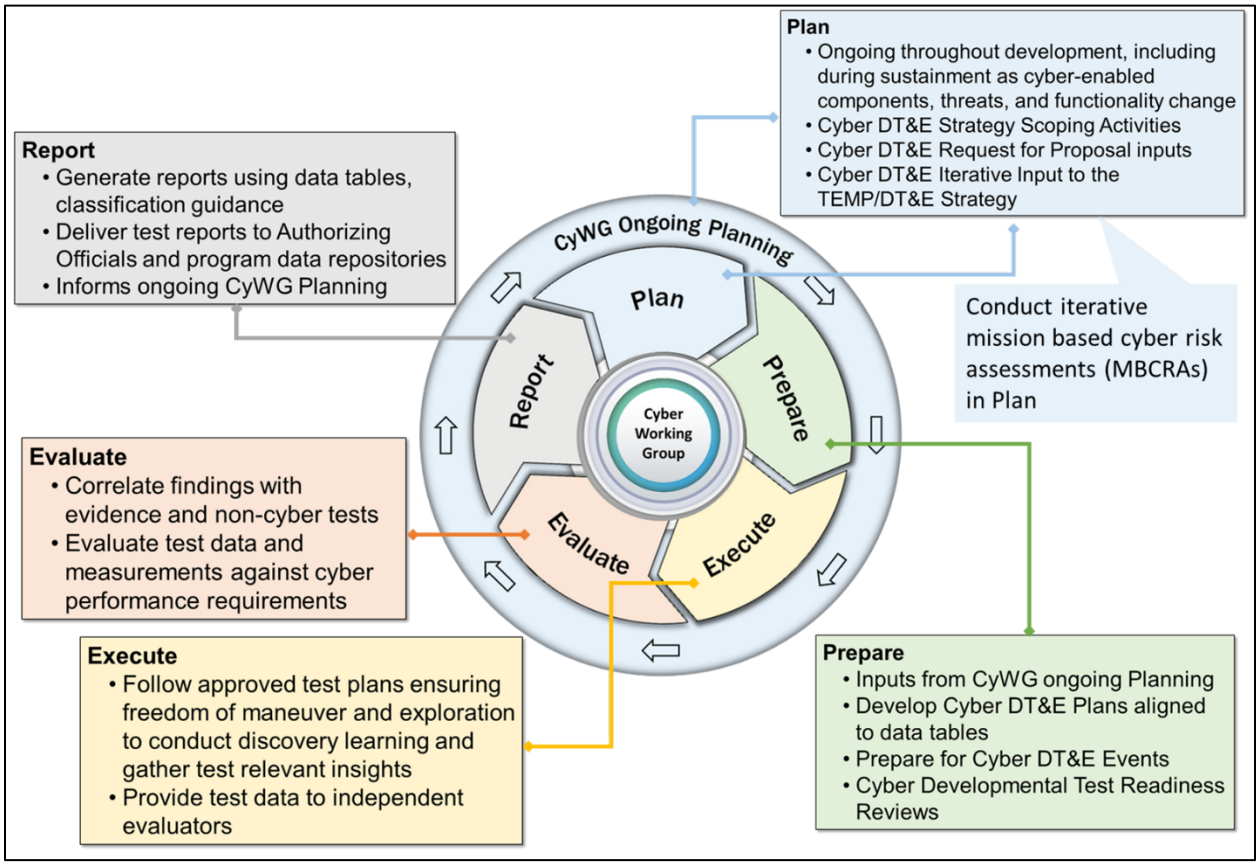


Figure 2-1. Cyber DT&E Iterative Process

The process in Figure 2-1 depicts a circle to represent iterative testing addressing new or emerging threats, test-fix-test approaches to verifying requirements, and testing to assess performance in evolving operational environments. The CyWG is at the center of the entire process. Common examples of events driving the repetition of activities and tasks include those in Paragraph 3.2.a.(13) of DoWM 5000.103. The outer ongoing planning circle represents a continuous CyWG process to support the iterative testing.

2.1.1 Iterative and Recursive Nature

Digital systems are complex and sensitive to change. Minor changes in software or configurations can have significant impacts on the risk posture of a system, jeopardizing its cyber resilience. To prevent such deficiencies, DoWM 5000.103 requires integrating cyber DT&E early and consistently through system maturation and keeping developmental pace with the SUT. The CyWG should scope iterative planning, preparing, executing, evaluating, and reporting activities and tasks at multiple points during a system life cycle, either chronologically or event driven. This process is not strictly linear, with many sub-activities occurring in parallel (e.g., while personnel are evaluating test data and measurements against cyber performance requirements for one event, the CyWG could also prepare for a test readiness review (TRR) to support another event). This parallel execution allows for a more efficient use of resources and a faster completion of the overall cyber DT&E process.

Figure 2-2 depicts the iterative and recursive nature of the cyber DT&E process.

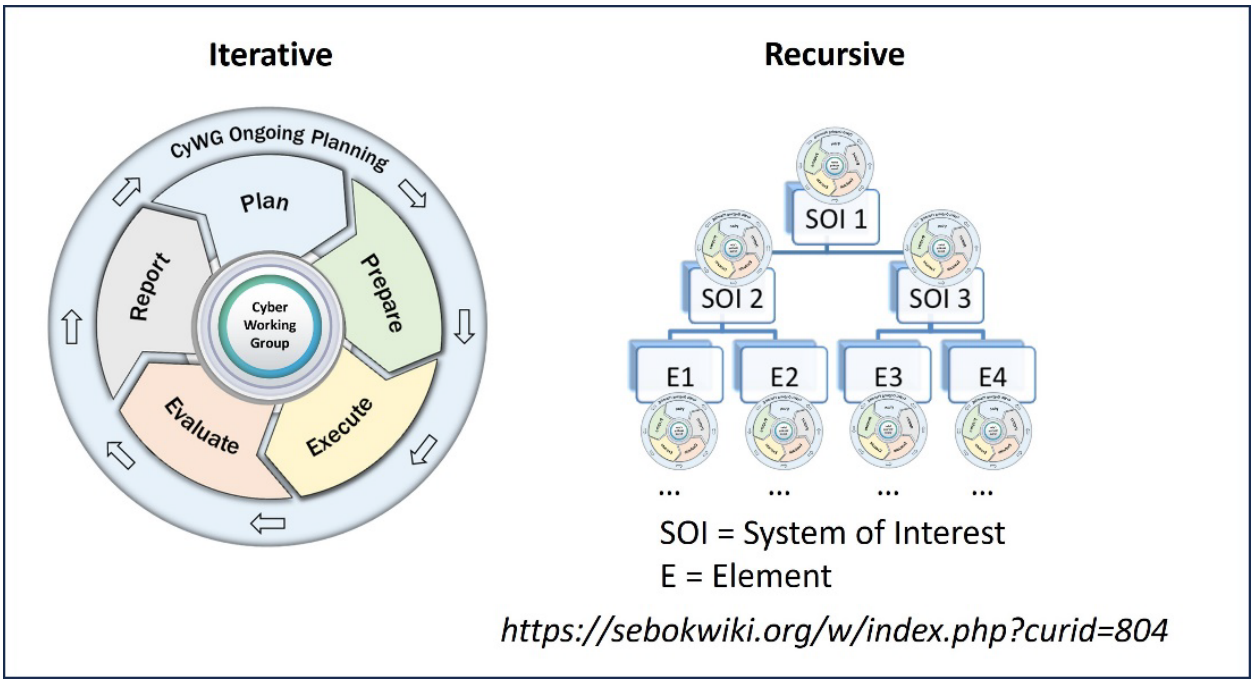


Figure 2-2. Cyber DT&E Process Is Iterative and Recursive

In Figure 2-2, the image on the left depicts the cyber DT&E process, and the image on the right shows that cyber DT&E is recursive, meaning that the system developer should reapply the cyber DT&E process to the decomposed subsystems and elements (components and subcomponents). The iterative process applies to each system of interest on each level. The recursion updates and expands the evidence base for verification judgments throughout system development.

Sections 3 through 7 of this guidebook provide additional details about each of the activities.

2.1.2 Tailoring Cyber DT&E for S&T, Pre-Acquisition, AAF, or Service-Internal Approaches

PORs are not the only construct for delivering capability to the warfighter. Multiple structures with different goals and contractual approaches are available to achieve specific ends. However, the fundamental steps relevant to cyber design and cyber DT&E activities should be consistent across all these different constructs. DoW conceives systems to achieve a mission within the operational context of threats and existing systems and missions.

The depth and extent of the cyber-resilient design required to meet a particular resilience need will vary for different missions, systems, and technologies. Three things govern those factors: (1) the intended longevity of a system, (2) the mission criticality of the computational elements, and (3) the anticipated lifespan and subsequent life cycle replacement of system components.

Example Requirement

The mean time to failure could be a reliability metric to predict the average time that mission-essential systems should operate before failure. This metric in cyber test planning provides insights into the expected reliability and lifespan of components, which is essential for effective risk management of mission-essential systems and subsystems. Cyber test teams could simulate cyber effects in a concurrent cyber and reliability test event to demonstrate how successful attacks could reduce the SUT mean time to failure, revealing vulnerabilities that compromise the previously verified reliability of mission-essential systems and subsystems.

Regardless of the pathway, if a mission- or safety-critical function in the system is allocated to computational hardware, software, or firmware, then there is a need to ensure the mission against faults and failures of those systems. As a result, the CyWG should plan cyber DT&E more rigorously for these components.

The organization developing the systems should address the cyber DT&E regardless of where the system is in the life cycle. Some systems may be well into the life cycle when cyber DT&E is reinitiated, which may include programs in sustainment. Accelerated acquisition programs may not have adequate time for the full recursion; however, the program manager should devote time, resources, and funding for early planning to inform the integration of system developer and

government cyber testing and identify a process (including understanding the cyber requirements and characterizing the surface) to establish the foundation for recurringly and efficiently verifying the system's security compliance, functional cybersecurity, and cyber resilience capabilities. Section 8 provides additional cyber DT&E considerations for different system developments.

2.2 Cyber Working Group

The primary execution entity for cyber T&E is the CyWG. The CyWG operates under the program manager's authority and coordinates with external entities and other internal non-cyber entities. DoWM 5000.103 lists the CyWG's cyber DT&E responsibilities.

2.2.1 CyWG Formation and Authorities

The program manager charters the CyWG and assigns roles, responsibilities, and authorities to CyWG leaders to execute all assigned activities. Often, the CDT or T&E lead chairs or co-chairs the CyWG. The CyWG should include an integrated multidiscipline team from across the engineering, test, intelligence, and cyber communities. The program manager designates chairs or additional co-chairs as desired. In large acquisition programs, the CyWG may focus exclusively on cyber DT&E. The CyWG may be small, led by the SSE or Program Protection Plan (PPP) lead, and heavily overlap with SSE, program protection planning, contracting, and other functional efforts.

The CyWG supports the T&E working-level integrated product team (WIPT) or integrated test team (ITT). The CyWG will coordinate, deconflict, and schedule support for the cyber T&E activities. Continuous collaboration among the other working groups and team leaders ensures successful cyber DT&E and the opportunity to design and develop a more secure and resilient system, regardless of the size of the effort.

Figure 2-3 presents a notional charter outline for the CyWG. The CyWG should tailor the charter outline as appropriate for the organization.

CYBER WORKING GROUP (CyWG) CHARTER OUTLINE
(Tailor as appropriate)

1.0 INTRODUCTION
1.1 AUTHORITY
1.2 BACKGROUND & PROGRAM/PROJECT DESCRIPTION
1.2.1 PROGRAM/PROJECT INFORMATION

2.0 CyWG MISSION, SCOPE AND OVERARCHING GOAL

3.0 CyWG GOVERNANCE

4.0 CyWG OBJECTIVES

5.0 CyWG MEMBERSHIP AND RESPONSIBILITIES
5.1 CyWG CHAIR
5.2 PROGRAM/PROJECT MANAGEMENT OFFICE
5.3 OPERATIONAL TEST AGENCY
5.4 LEAD DEVELOPMENTAL TEST & EVALUATION ORGANIZATION
5.4.1 SUB ORG 1
5.5 OPERATIONAL USER ORGANIZATION
5.5.1 SUB ORG 1
5.5.2 SUB ORG 2 – OPERATIONAL USERS
5.6 JOINT INTEROPERABILITY TEST COMMAND (
5.7 SERVICE T&E ORG
5.8 OFFICE OF THE SECRETARY OF DEFENSE (OSD) OVERSIGHT
5.8.1 DIRECTOR, OPERATIONAL TEST AND EVALUATION
5.8.2 DIRECTOR, DEVELOPMENTAL TEST, EVALUATION, & ASSESSMENTS
5.9 ASSISTANT SECRETARY OF THE [SERVICE]
5.10 US GOVERNMENT EXECUTING OR PARTICIPATING TEST ORGANIZATIONS
5.10.1 [TEST ORG 1] (CYBER DT&E, LFT&E, OT&E ORGS)
5.11 CONTRACTOR TEST ORGANIZATION(S)
5.11.1 [CONTRACTOR/OEM] TEST & EVALUATION

6.0 FORMATION OF SUBGROUPS
6.1 TEMP/T&E STRATEGY WRITING TEAM
6.2 CYBERSECURITY ASSESSMENT AND AUTHORIZATION SUBGROUP
6.3. INTEROPERABILITY CERTIFICATION SUBGROUP
6.4 IOT&E READINESS CERTIFICATION SUBGROUP
6.5 LFT&E ASSSESSMENT SUBGROUP
6.6 PROGRAM PROTECTION EVALUATION SUBGROUP
6.7 TEST DEFICIENCY MANAGEMENT SUBGROUP
6.8 THREAT AND INTELLIGENCE SUPPORT SUBGROUP

7.0 PROCEDURES AND ADMINISTRATIVE MATTERS
7.1 CyWG MEETING FACILITATOR/SECRETARIAT
7.1.1 MEETING MINUTES
7.1.2 ACTION ITEMS
7.1.3 ATTENDANCE
7.2 FREQUENCY OF MEETINGS

8.0 CyWG CHARTER UPDATES

9.0 COORDINATION AND SIGNATURES

10.0 CONFLICT RESOLUTION

Figure 2-3. Notional CyWG Charter Outline

2.2.2 Recommended CyWG Participants and Roles

Figure 2-4 depicts the recommended CyWG participants. CyWG participation and specific responsibilities for a particular role may change over the course of the system life cycle. See Appendix A: for details on additional considerations for staffing cyber DT&E activities.

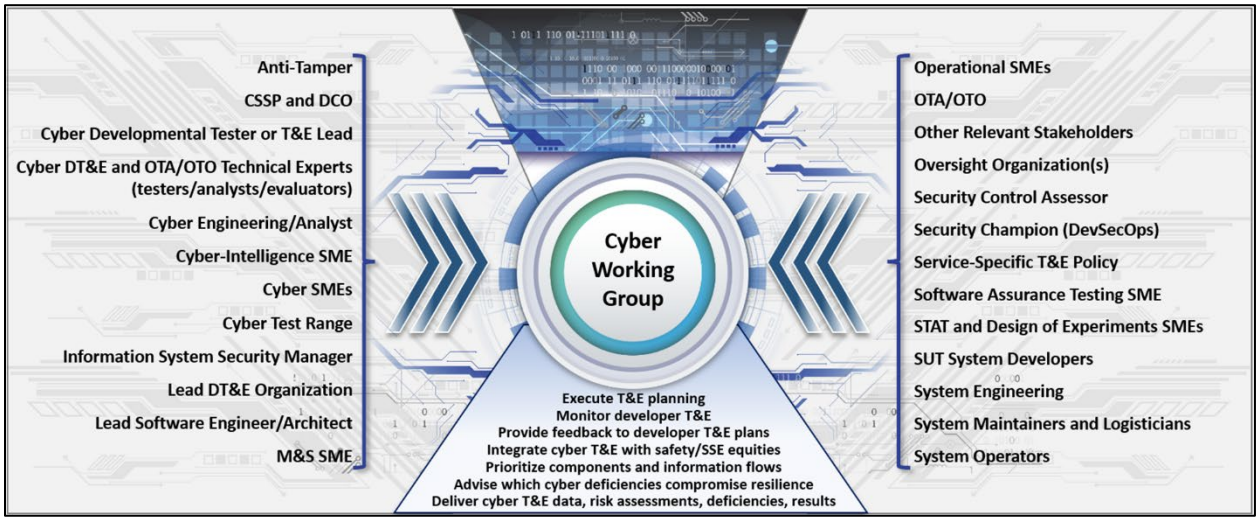


Figure 2-4. CyWG Representatives and Responsibilities

2.2.3 Documentation, System-Relevant Artifacts, and Data Management to Support Cyber DT&E

The CyWG is the focal point for capturing cyber DT&E–related equities in all documentation and activities. Appendix C: includes a list of acquisition program documents that the CyWG should help develop, influence, and use in planning cyber DT&E activities.

2.2.3.1 CyWG and Cyber DT&E Intersection with Program Protection

One document of critical significance to cyber DT&E planning is the PPP (or a similar document if the AAF pathway does not require PPP development). The SSE team (see Section 2.5) develops and maintains the PPP, which identifies the missions and critical functions and describes the technological advantage elements; the critical technology elements consistent with hardware and software assurance; and the system's critical components essential to mission success. The PPP describes the criticality analyses (see Section 3.3.4) and consequences of losing mission capabilities in terms of mission impact levels for specific components.

DoD Technology and Program Protection Guidebook

Cyber DT&E processes should integrate with other required security and protection efforts explained in the DoD Technology and Program Protection Guidebook:

https://aaf.dau.edu/storage/2024/08/TPP_Guidebook.pdf

The Program Protection Implementation Plan (PPIP) describes how the system developer's design meets the PPP requirements, including information and communications technology (ICT) supply chain risk management (SCRM) and hardware and software assurance. The CyWG should plan cyber DT&E events to verify the hardware and software protection requirements, including anti-tamper (AT) and those requirements described in the PPP and its appendices, and implementation of the protections described in the PPIP, including verifying the security of the system development environment and system development processes. The CyWG coordinates with the DoW Executive Agent for AT (See Appendix L for additional information).

The following list describes the interaction between the CyWG, contract team, SSE team, and test teams in relation to test, program protection, and cyber requirements:

- Developer test teams should focus testing on critical components to evaluate the risk to the mission in contested cyberspace through concurrent cyber and non-cyber tests.
- After testing, the DT&E test lead provides the SSE team with test results.
- Test results may lead to refining requirements or engineering changes to mitigate program protection risks, including initiating contract actions.

2.2.3.2 Data and Documentation Access and Management

The CyWG should coordinate with the program manager on the procedures and infrastructure to provide T&E stakeholders with access to all cyber DT&E–related data at all relevant classification levels. The CyWG should determine whether the program manager and other participating organizations already have a data management plan and infrastructure before seeking independent procurement or development of databases and other repositories.

Data Correlation and Reporting Solution

The program manager or system owner should consider adopting a data correlation and reporting solution (e.g., Splunk, Amazon S3 bucket, Microsoft Azure Data Lake). These scalable data storage and analytic services for big data applications offer platforms for searching, storing, and advanced data analytics.

Besides cyber DT&E data, the CyWG should consider the stakeholders' needs for access to system data and other types of T&E data, which will require coordination with groups outside the CyWG itself. The CyWG should assist the program manager in ensuring that government data rights enable the inclusion of developer test data, including commercial cloud data, in the program's accessible databases. The CyWG should understand the types and formats of the expected data to define the scope and requirements for a storage and management infrastructure.

The CyWG should coordinate cyber resources across the program manager's organization and system developers to establish and curate the test data repositories. Specific issues that the

CyWG should address include the protection of proprietary information, classification by compilation, actively managing permissions/access and groups, access to the "right" networks, availability of specific tools (some of which require licensing or specific expertise), and curation of the data itself. The process of discovering test-relevant data within a massive system developer's repository should not seem like "dumpster diving," where satisfying simple requests for information (RFIs) takes weeks, but should be part of a well-thought-out test strategy. By actively coordinating and developing a cyber test data repository requirement early, the CyWG can facilitate knowledge management and curation of data, amplifying the T&E effectiveness and efficiency.

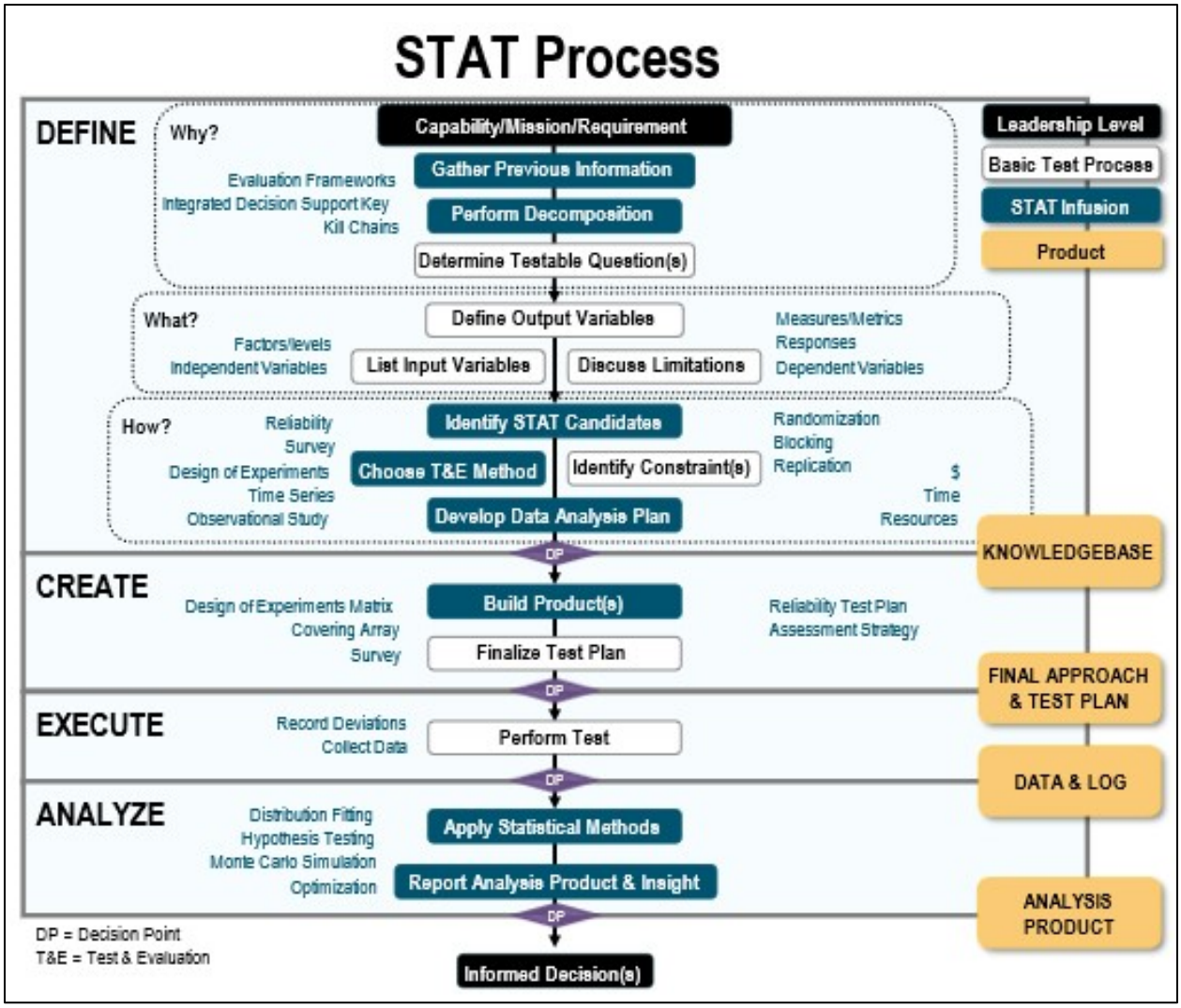
2.3 Early CyWG, Test Team, and Analyst Involvement

DoWM 5000.103 stipulates that the S&T or program manager will provide resources and confirm schedules across the system life cycle to enable the cyber DT&E process. Involvement in contract considerations is the first component of planning for cyber DT&E, and the CyWG should assist in developing contract language as early as possible. Including the CyWG, cyber test team, and analyst at these preliminary stages enhances the effectiveness of the *Planning* activities in Section 3 and saves the organization from the cost and delay of adding cyber requirements and cyber testability requirements later in design.

2.4 Role of Scientific Test and Analysis Techniques in Cyber DT&E

Scientific test and analysis techniques (STAT) are the scientific methods and processes used to develop efficient, rigorous test strategies yielding defensible results. To improve test rigor and inform decision making, the CDT or T&E lead should recruit STAT personnel to consult with the CyWG on test planning, test execution, and analysis. The STAT process, depicted in Figure 2-5 is a deliberate test-planning methodology focused on the application of STAT. It lays out a logical flow for determining what STAT is most applicable to any given situation or domain (including cyber). The figure depicts the STAT process as a sequential flow, and although it is very cyclical, it allows test teams to break the flow at any point and go back to any previous phase.

The STAT process has four phases known as define, create, execute, and analyze. Each of the phases ends with a decision point where the test team assesses the products of each phase to determine whether to move on to the next phase, go back to a previous phase (if information from a previous phase has changed), or exit the process entirely. The STAT process facilitates rigorous testing in the cyber DT&E process by quantifying risk, defining the test space, and guiding stakeholders to develop analysis products designed to address requirements.



Source: STAT Center of Excellence

Figure 2-5. STAT Process

Bounding and controlling risks of attacks and exploitation requires a strong understanding of their rates of occurrence and detection, and these data are not often available or reliable for cyber. STAT provides rigorous test design and design evaluation methods to understand the likelihood of collecting the required data and designing the test to collect the correct data efficiently. Structured test designs allow test teams and analysts to draw cause and effect conclusions between input variables and output variables because of the control placed on sources of variation. The conclusions enable the quantification of risk, characterization of consistent occurrence and response rates for cyber events, or determination of the impact that the number of users or network configurations has on cyberattack detection and response.

A covering array is a combinatorial test design method used to quantify test coverage and provide guaranteed coverage of factor combinations to a chosen degree and quantified coverage

at higher levels. Covering arrays are particularly useful for designing tests to ensure known coverage for negative testing, dynamic software testing, and combinatorial fuzz testing. For example, using a covering array can demonstrate whether a firewall port configuration behaves as expected and allows only authorized traffic by calculating a proportion of unauthorized traffic test cases blocked by the firewall. Statistical modeling supports inference using logistic regression to compare false positive and negative rates, such as between two potential authentication methods.

Statistical modeling of failure distributions or producing seasonal modeling establishes system trends and predicts system behaviors based on reliability metrics. STAT can quantitatively assess cyber resilience through a combination of component reliability and survivability estimates, system availability, and reliability block diagram analysis to quantify combined survival probability and mission resilience.

STAT enables insight from data to decision. The CyWG can use STAT to:

- Apply statistical modeling techniques to perform inference on cyber test data.
- Reduce resource demands on formal testing, saving resources for free play.
- Create structured test designs that reduce and quantify the risks of insufficient testing.
- Evaluate the risk of mischaracterization of data based on insufficient test times.
- Inform the question of how much cyber testing is enough.

Tailored STAT can support efficient, rigorous, and focused cyber DT&E. The CyWG should include a STAT team member to ensure the best application for cyber DT&E. Contact the STAT Center of Excellence for additional information via https://www.afit.edu/STAT/.

2.5 Cyber DT&E Relationship to System Security Engineering

As described in DoD Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage," SSE focuses on the protection of the critical technical information and critical program information (CPI). This includes safeguarding sensitive details such as a program's existence, platform characteristics (range, speed), and novel system capabilities such as information vital to maintaining a technological advantage. Section 3.5 of the DoD Technology and Program Protection Guidebook further emphasizes mission-critical functionality within the context of trusted systems and networks (TSN). While a highly assured system should be functional in its mission environment, trade-offs may be necessary, potentially accepting risk to CPI for the sake of mission accomplishment. To ensure informed decision-making, the CyWG and SSE working groups should compare design inputs and resolve

conflicting priorities, with program managers seeking appropriate guidance when proposing the acceptance of risk to CPI and ensuring horizontal protection of sensitive technologies.

DoDI 5000.83; DoDI 5000.89, “Test and Evaluation”; and DoWM 5000.103 collectively require the test community to verify that the system can perform its critical functions in a realistic cyber environment. This verification includes measuring and evaluating specified cyber performance requirements for the system’s ability to prevent, detect, contain, mitigate, or eliminate, and recover from the loss of mission, or safety-critical functions within required mission timelines. The CyWG is responsible for defining these testable measures as part of test plan development and test requirements. Feedback from cyber DT&E informs system developers, ensuring they’ve incorporated resilient design practices and sufficient cyber protections into the foundational system design, and helps implement appropriate risk mitigations.

3 Iterative Planning for Cyber DT&E

Planning, in the context of this guidebook, is not the sequence of activities leading to a test plan (which is during *Preparing*); *Planning* is the strategic set of activities that continuously examines and advises on system requirements and organizes and scopes the subsequent test event(s), time sequencing, execution, evaluation, reporting, etc. Several foundational activities and considerations remain relevant throughout the conduct of cyber DT&E. Section 3 activities may be a continuous CyWG evolution of revisiting and updating the activities as explained in the following subsections; depicted in Figure 2-1; and described in DoWM 5000.103.

3.1 Cadence

The CyWG should conduct *Planning* activities in a continuous cycle, informing the *Preparing*, *Executing*, *Evaluating*, and *Reporting* activities, while incorporating data and feedback from each of those activities into the overall cyber DT&E strategy. The CyWG should review the data and results of each activity and use this information to inform future activities of the cyber T&E process. The CyWG should recurringly update the cyber DT&E strategy to evaluate cybersecurity and cyber resilience risk to address changes as outlined in Paragraph 3.2.a.(13) of DoWM 5000.103.

Schedule alignment should begin as early as possible for non-acquisition, pre-acquisition, and acquisition pathway timelines and should include collaboration with the engineering design team. Early alignment establishes a baseline, informs strategies, and aligns testing to inform decisions, support *Preparing* activities, and evaluate overall progress.

Scheduling Long-Lead Items

Scheduling should ensure a focus on long-lead items, such as flight-safety clearance for certain tests, shipbuilding installations, VV&A work to enable tests against non-production assets, lab/ground/range time with SUT and appropriate stimulus, etc. Each of these items can delay delivery by demanding wait time for requirements verification.

Planning activities for cyber DT&E should align with system development, providing timely and actionable improvements. Test timing should align with the availability of modeling and simulation (M&S), mature-enough SUT functionality, and lulls in development changes and should avoid critical path schedules. This early test planning and execution alignment allows developers to easily remediate findings in the system. Because cybersecurity and cyber resilience span the entire system (hardware, software, firmware, etc.), and vulnerabilities can emerge at any point in time, the CyWG will prioritize the SUTs for repeat testing as different components mature at different rates (e.g., when the chosen implementation is a hardware security kernel reporting information through a firmware pathway to alert an operator or satisfy a log

requirement). M&S mimicking system behaviors can enable cyber DT&E before physical components are complete.

Kitchen Line Check

A useful metaphor is a commercial kitchen. The chefs prepare and review the order before it leaves the kitchen for delivery to the customer. It is much easier to verify the quality and safety of food preparation before the food leaves the kitchen than it is to re-execute the entire plate after making a bad dish.

In development, security, and operations (DevSecOps), scheduling and testing are a continuous challenge for practitioners because of the effect on velocity when mismanaging cyber DT&E. It is often more effective to put effort into evaluation versus attempting to use tests to verify a minimum viable product. The CyWG should consider shifting earlier in development and integrating deeper into development teams to ensure that user stories (for example) are testable and verify DT&E requirements. Furthermore, test teams should strongly consider requesting evidence of software assurance practices and security-related design features (e.g. when the application requires the Internet to provide microservices, which carries a risk of pollution).

Kitchen Inspection/Certification

Again, the metaphor of a commercial kitchen is helpful. As in DevSecOps, the program managers want to quickly deliver a number and variety of high-quality products. The Health Department certifies the kitchen itself, inspecting the ability of the kitchen staff to create safe food from safe ingredients using hygienic processes. The inspectors lack the resources necessary to examine each dish from every kitchen separately.

As an example, examine the case where a DevSecOps pipeline produces a new product every 5 weeks. If the legacy T&E process takes 6 months to complete, then testing is constraining the "velocity" of the pipeline (the speed at which it can deliver new capability). But by integrating with the security practices of the pipeline itself before code development; understanding the automated test approaches; and verifying that the pipeline tools, processes, and environments meet the security requirements, the CyWG can characterize the risk to the software-supported mission based on assessing the effectiveness of the pipeline components implementing secure coding practices.

3.2 Inputs

As *Iterative Planning for Cyber DT&E* activities and tasks occurs along with the development, the documentation will evolve and provide more information either for the context of testing or the conduct of testing, evaluation, or assessments across multiple data sources. Appendix C: provides many of the key system artifacts to support cyber DT&E. As explained in Appendix G: MBCRAs will require similar documents. The organization should maintain configuration control in a repository and provide authorized access to the documentation. Alternatively, if the organization is using digital engineering (DE), the system models will enable access to this authoritative source of truth required for cyber DT&E planning.

CyWG participants should know how and where to get information and what data and documentation is in the repositories to minimize artifact-retrieval burdens and not restrict the progress of cyber DT&E (e.g., if the organization has a different or incomplete set of documents). Example inputs for *Planning* may include:

- Capability requirements documents: Joint Capabilities Integration and Development System (JCIDS) (or Component-level requirements processes) Initial Capabilities Document (ICD) or Capability Development Document (CDD), or other documents capturing overall capability requirements (including context).
- Mission concept of operations (CONOPS).
- Cyber Survivability Risk Category from the Cyber Survivability Endorsement Implementation Guide process.
- System functional requirements.
- PPP: including criticality analysis, software and hardware assurance, ICT supply chain and AT requirements, and cybersecurity strategy (CSS) (DoW or Component Chief Information Officer (CIO)-approved document).
- Systems Engineering Plan (SEP).
- DoD Architecture Framework (DoDAF) System Viewpoints (SVs) or model-based systems engineering (MBSE) artifacts.
- Design specifications (if available).
- DBS Capability Implementation Plan (if available).
- Validated Online Lifecycle Threat (VOLT) Report, cyber threat modules from the Defense Intelligence Threat Library (DITL).
- Security classification guide (SCG).
- DoW RMF Security Plan, DoW RMF Security Assessment Plan (SAP).



- Past MBCRA results, if available.
- Prior test results, if available.

See Appendix C: for additional information.

3.3 Activity: Cyber DT&E Strategy Scoping

The cyber DT&E strategy scoping activity consists of various tasks designed to obtain input from relevant stakeholders, perceive their priorities, and pinpoint the dimensions of the pending

cyber DT&E strategy scoping activity. This activity concentrates on shaping and refining attainable cyber DT&E objectives (e.g., prioritization of SUTs, establishing schedules for data-driven decisions, and ensuring verification of required cyberspace performance).

3.3.1 Task: Examine and Advise on Cyber Requirements

Acquisition programs, regardless of AAF pathway, should have defined cyber functional and performance requirements. Non-acquisition or pre-acquisition projects should also have defined cyber performance/functional requirements. The CyWG should ensure that the cyber requirements make sense within the context of the mission(s) (including protection of information and mission assurance in the face of exploitation); are measurable and testable; and are implementable by one or more design choices in architecture, specification, or implementation. These design choices are the primary mechanism to achieve acceptable residual risk and may take the form of:

- Operational resilience requirements expressed through design (required by DoDI 8500.01, "Cybersecurity").
- Cyber survivability requirements (i.e., the Joint Staff's Cyber Survivability Endorsement).
- Testable requirements for point applications of controls, such as DoW RMF technical controls and Security Technical Implementation Guides (STIGs). Some DoW RMF security controls (e.g., organizational policy and governance controls or controls specifying testing or training) are not performance requirements.



DT&E events verify the satisfaction of technical performance requirements for DoW systems. The CyWG has the responsibility to test (control, stimulate, observe) and evaluate (collect, analyze, judge) cyber for the SUT, as expressed in the requirements but also as expressed in the system architecture, specification, and implementation choices. An external document or external standard by itself is not a performance requirement. Procurements that are not traditional JCIDS acquisition programs usually have implied cyber requirements that the SE team needs to specify or derive. The CyWG should strive to ensure that top-level cyber performance requirements are measurable and testable with defined threshold levels based on the mission(s). The initial MBCRA should be used to help the CyWG provide input to the SSE team for decomposed cyber requirements.

The contract should require the system developer to verify requirements before delivering the product to the government. The government should provide system technical requirement specifications to the system developer as part of the contract. The system developer decomposes and implements the requirements into the engineering detailed designs (models if using MBSE) and then verifies them during system developer–led cyber testing. Government DT&E organizations verify functional cyber performance requirements during acceptance cyber T&E and during government cyber DT&E. The government may choose to accept system developer test results for the purpose of requirements satisfaction but should pay careful attention to the conditions under which the system developer collected the data and the limits of what those data substantiate.

Decomposed System Requirements

Decomposed requirements should be measurable, testable, and achievable. The CyWG should request the requirements verification and traceability matrix (or similar documentation) to confirm the traceability for cyber requirements. This matrix can help track system developer cyber DT&E and other verification activities (demonstration, examination, analysis, and test). See Appendix B: for more information.

If the SUT has a System Survivability (SS) Key Performance Parameter (KPP), then the CyWG should support the acquisition program's SSE team in defining the technical requirement specifications from the cyber survivability attributes (CSAs). The team should examine applicable CSA requirements as described in the ICD or CDD. The CyWG also examines, analyzes, and documents if and how the SSE team engineered operational requirements into the system design to support the SUT's requirements to resist, absorb, and recover from or adapt to adverse conditions, stresses, attacks, or system compromises. The CyWG can derive cyber requirements from CSAs and mission-essential functions required for successful mission accomplishment in modern contested cyber environments (persistently strongly contested).

Reviewing Requirements

The CyWG and test teams should ask:

- How completely are the cyber requirements documented?
- Does the system effectively integrate and balance cyber requirements with other requirements and KPPs?
- Where are the requirements kept?
- Are the requirements sufficiently detailed? Is the specified standard derived to a testable requirement? ("Resistant from all known and future malware" is NOT a testable requirement.)
- What is the most effective verification method?
- Are the chosen test tools capable of obtaining the data needed to verify the requirement?
- What verification methods are suitable for each requirement?

3.3.1.1 Testability Requirements for Cyber

Carefully constructed testable cyber requirements should be related to functional requirements. STAT experts can assist with the review of the requirements for testability. Testing is the process of controlling the environment, stimulating the system, and observing the results. A test report, to be worthwhile, should draw a clear and repeatable cause and effect. Systems designed in such a way where effects are not traceable to causes, or lacking the necessary level of introspection, are significantly harder to execute test events on and deliver meaningful assessments. A best practice is to resource the sustainment of a cyber test article enabling reliable and repeatable introspection and data collection, either permanently or temporarily (during development).

3.3.1.2 Testing Cyber Resilience as a Component of Operational Resilience

T&E of cyber resilience as a component of operational resilience relies heavily on the holistic connection between cyber and SE of the entire system. The operational resilience of the SUT is in the context of a mission, so test teams should construct mission-relevant measures. The system functionality required to achieve the mission drives the test points and setup, so the test points should be functionally relevant. Test teams should be able to explain the connection between an individual requirement and the residual risk to an operational mission.

For example, the requirement is "the system must provide a response time less than 1 second, given a flood condition greater than 120 percent of designed socket opening requests, sustained over a period of time exceeding 30 seconds." The team is accountable for corroborating this threat as a genuine denial-of-service attack originating from the designated adversary, at the specific time, for the observed durations. Should the need arise, the test team can resort to employing STAT to create a complete and practical array of representative threats. The test team will need to devise measures (anchored on the system response time) and the data collection and instrumentation (e.g., what points to measure between and other time-related property measures). The test team will have to abstract away defensive cyberspace operations (DCO) capabilities because DCO was not a part of the requirement or the specified operational environment.

Applying STAT

STAT may provide or help craft documentation of test responses, factors, levels, known covariates (measured and unmeasured), the test design methodology and rationale, and the matrix of planned test points. STAT may also help the CyWG and test team understand the limitations of testing in terms of the number of variables possible versus the amount of time available.

The test would then place the instrumented SUT into the desired configuration and stimulate it with the traffic representing the valid threat profile. Testing may be a combination of cooperative (assume compromise at a particular point, e.g., white-box testing) and adversarial (adversary establishes access and builds an effects chain, e.g., black-box testing) approaches or both. The test team runs the operational scripts and gathers data on system response time while under the load, which is both nominal traffic and threat inputs. The evaluation is then whether the system met the requirement in a sufficient diversity of conditions to judge that the operational resilience requirement is satisfied. The cyber DT&E team may also coordinate the test event and set of points with the OTA/OTO. Some systems may revert to a temporary shutdown when faced with the test approaches. Some systems may revert to a lower-bandwidth mode or some sort of port hopping. Test teams should have sufficient design and implementation information before testing, so there are no surprises by the SUT response, although test escapes sometimes happen. The measures of resilience should take those response options into account (e.g., is it sufficient to calculate an average uptime, including resets? Or is any delay longer than X seconds unacceptable?).

The test plan may include assessing the response when the test team attacks the system directly or when the system is in a threat-responsive state based on an external dependency. Test teams should be diligent to observe SUT boundaries while ensuring focus on the risks related to information exchanges. The authorization boundary is relevant only when the test event itself impinges on the authorization certification boundary. The CyWG and test teams should ask themselves the following questions:

- Is there a well-documented connection between the individual cyber nonfunctional property, the cyber-allocated function, and the operational mission context?
- Did the cyber T&E representatives have visibility on the operational resilience requirements? Was there an early influence on feasibility and testability?
- Is there potential operational test (OT) value in this test, without driving the test outside the specified value and conditions?
- Are the characteristics of the attack validated?
- Is the SUT response sufficiently well-documented to characterize how the SUT performs under a challenge?

- Are requirements structured in a way that helps complete the T&E events?
- Do the tested conditions accurately represent the specified threat? If requiring threat validation, how much time has passed since defining the requirement?

3.3.1.3 Testing Cybersecurity Standards



Cyber DT&E teams (system developer or government) may test and verify the implementation of DoW RMF technical controls (once applied) and then evaluate (before application or in lieu of direct testing) the effectiveness of the controls. Nontechnical or process controls are difficult to test in a component/network mindset, and a resilient design will present additional difficulty to a chain of malfunctions seeking to defeat a mission. Therefore, for nonmaterial controls and mitigations, the CyWG and test teams should consider evaluation versus testing.

Security control assessors and AOs should coordinate with the T&E activities supporting a program manager to gain additional information on the utility of controls applied and positive design features of a system that may not align to the taxonomy of the DoW RMF.

Application of security controls, in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Information Systems and Organizations," should be the final addition to system implementation, undertaken at the end of a security-integrated system design approach.

3.3.2 Task: Examine Current Threat Assessments



An assessment of cyber threats should scrutinize each element that may bring about mission performance failures. Designing and testing a system without understanding the relevant cyber threat may result in system weaknesses or exposures that a human or automated process could exploit. The CyWG should consider system use in an unintended manner to cause mission performance failures. It is critical to involve intelligence subject matter experts (SMEs) in this discussion to identify accurate threat intelligence for the specific system. The CyWG recommends an appropriate frequency for conducting cyber threat assessments throughout the system development life cycle, but at a minimum, acquisition programs should obtain a validated threat assessment (e.g., VOLT Report or Service/Component threat assessment report) from the Defense Intelligence Agency (DIA) at each decision point. The program manager's organization is responsible for evaluating and updating the MBCRA and DoW RMF risk assessment, if necessary, using updated threat assessment information. The CyWG's prioritization of deficiency reports (DRs), watch items, and test findings benefit from familiarity with not only current threat reporting but also trend information about adversary capabilities development and strategic goals.

The CyWG should ask these questions:

- If it is an acquisition program: Who is the intelligence support to the acquisitions branch? How do I get in contact with them?
- If it is not an acquisition program: What intelligence support does this evaluation and reporting require? How would I get it?
- Can the test team hear, process, and store, relevant information at the right classification levels? Does the classification level change post-test after confirming or refuting a hypothesized problem?
- Does the test team interface with its intelligence support to increase the focus of reporting or help formulate collection requirements?

See Appendix D: for a detailed explanation of how to employ the intelligence community (IC), use IC cyber threat analysis TTPs, obtain cyber threat assessments, and obtain IC support for cyber DT&E events.

3.3.3 Task: Characterize the Attack Surface

The CyWG should characterize the "attack surface" (which is bigger than just attacks—it includes all risk sources) for every information flow into and within the system. Identification by information flow and not components helps later when single components host multiple functions and flows.

Terminology

An **attack** is a directed action or series of actions taken by an adversary, or an unwitting actor, with the result of compromising a system's mission by exfiltration, infiltration, or manipulation of information, data, or code.

The attack surface characterization relies upon a decomposition analysis, including the mission-relevant terrain in cyberspace, and then the evaluation of every possible information flow path. This process determines (1) the mission impact of a malfunction, pollution, or exploitation at each flow point and (2) what prevents a malfunction from entry, exploitation, and exfiltration of system data with the goal of potentially disrupting mission and system operations. The CyWG will also examine the attack surface from the perspective of adversary action. Adversary objectives may include the compromise of confidentiality, integrity, availability, nonrepudiation, or other security-relevant properties of the information exchange.

DoWM 5000.103 provides a list of evolving attack surface elements that may apply to various information flows, networks, subcomponents, components, or subsystems in the SUT. Appendix E: provides more information about the attack surface characterization.

3.3.3.1 Information and Communications Technology Supply Chain

Characterizing the ICT supply chain as an attack surface to inform cyber DT&E scope is a major task as part of the attack surface characterization; see Appendix E:. Appendix F: provides additional information on ICT supply chain considerations when planning cyber DT&E for ICT supply chain risks.

3.3.3.2 Analyze the Attack Surfaces

For every information flow, the CyWG should determine the mission impact on the SUT. The CyWG should identify the information flow boundaries, including the trust relationships among functional subcomponents and the specific information flows. The CyWG should assess which flows are vulnerable to accidents or adversaries to verify effective security measures. By pinpointing these vulnerabilities, the CyWG can enhance the protection of sensitive data and ensure that all components function within the defined trust parameters, improving the system's overall integrity. The CyWG should ask, "What happens if?" and determine, using the expertise available through the collected CyWG participants and stakeholders, all the potentially mission-killing system behaviors and the effectiveness of the preventive measures intended to reduce the unwanted behavior. MBCRAs help to perform this analysis, but the CyWG can analyze emerging attack surface risks at any point in the life cycle. The output products of this analysis directly feed subsequent analysis.

3.3.4 Task: Support Criticality Analysis

The DT&E and SE communities should closely collaborate during criticality analysis. SE artifacts serve as the authoritative reference source for documenting information flows and authorities within an objective system. Many organizations use digital artifacts, and cyber DT&E practitioners should have access to the tools and expertise to gain knowledge of system design.

The two most important divisions in SE for the cyber test team are at the functional allocation line—on one side should be a complete functional description of the system (i.e., what it does) and on the other side the full description of what components and software are allocated to execute those tasks.

It is possible to assess certain features of a system's security and cyber resilience simply by examining the information flows at the abstract level (a Unified Architecture Framework (UAF) "operational" viewpoint), even before selection of a materiel solution. The CyWG should identify high-interest items for T&E to influence the design (or at least highlight the risk) because the design choice inherently drives considerable risk.

Once physical or computational systems have been allocated to functions (the UAF "system" level), the architecture has and impact on the system's security and cyber resilience, and becomes part of a focus for testing—for example, if T&E identified the previous architectural design as being inherently risky, and the engineering team believes it is necessary to maintain the architecture for other mission reasons but allocates strong physical and procedural controls to achieve acceptable residual risk. Cyber DT&E will then be responsible for verifying the strength of the physical protections to inform overall cyber risk to the mission.

DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks"

This issuance defines criticality analysis and implements the DoW's trusted systems and networks (TSN) strategy through program protection and cybersecurity implementation to provide uncompromised weapon and information systems. It also defines TSN:

> A state of security of a system or network in which its functions and components that are critical to conducting the system's intended missions have been protected from intentional malicious insertion-related threats and attacks to an acceptable level of risk through the use of robust SE, SSE, ICT SCRM, security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines.

Cyber test team representatives should provide threat-relevant input to the criticality analysis highlighting mission-relevant terrain in cyberspace, providing the path to mission- and safety-critical functions and components.

3.3.5 Task: Conduct Mission Based Cyber Risk Assessments

DoDI 5000.89 and DoWM 5000.103 require iterative MBCRAs, which are an analytical, iterative process to identify, estimate, assess, and prioritize risks to DoW operational missions resulting from cyber events. The CyWG plans, conducts, or updates MBCRAs and includes representatives of the user community, the system designers, and a cyber technician with familiarity using cooperative or adversarial techniques.

MBCRAs should inform engineering, risk management, and the scope of cyber testing. MBCRAs help the CyWG prioritize the planning of cyber DT&E for subcomponents, components, and subsystems (SUTs) that may affect the mission(s) enabling the CyWG to avoid dedicating significant resources to the planning of cyber DT&E that does not affect the mission(s). For example, a port may show itself open during a port scan, but if abuse or exploitation of data through the port does not and cannot affect cyber performance requirements or the mission, then testing is of low priority. MBCRAs will mature alongside the development and throughout the life cycle. The CyWG should plan to periodically update previous assessment products to incorporate changes in design, environment, mission functionality, and threats to inform engineering, programmatic, risk management, test, and operational utilization decisions.

Refer to Appendix G: for comprehensive details on MBCRAs; their use in cyber testing, risk management, intelligence, and SE; and the responses to some frequently asked MBCRA questions.

3.3.6 Task: Use Prior Test Results

The CyWG uses prior test results to inform the cyber DT&E strategy and prioritization of SUTs for upcoming test events. The CyWG should understand and track current SUT problems, previous versions, test findings, and the test conditions. Previous testing on a common technology element subcomponent, component, or subsystem may exist in a different organization. The CyWG should ask:

- What T&E events occurred, and where do we gain the information?
- What other systems/efforts are using similar hardware or technology, and how would those work together?
- Does the test team have the right clearances and environment to receive the prior test reports/plans/etc.?
- Can the CyWG leverage information shared and connections made at cyber T&E working group meetings to avoid unnecessary repetition of a test or expand and learn from other discoveries?

3.4 Activity: CyWG Input to System Developer Contract Requirements

The CyWG should be significantly involved in the requirements definition phase of system development to ensure the inclusion of measurable, testable, and achievable cyber performance requirements that are relevant to the mission and to ensure that the requirements enable the required cyber testing. The CyWG should also ensure that the contract provides the provisions identified in DoWM 5000.103 for system developer cyber DT&E; system developer engagement in the CyWG and CyWG activities; and delivery of system developer cyber DT&E plans, data, and results. The CyWG should ensure the contract includes requirements for the provision of data artifacts, test articles, and M&S representations. See DoWM 5000.103 and Appendix I: for additional provisions and considerations.

3.5 Activity: Cyber DT&E Iterative Input to the TEMP or T&E Strategy

The TEMP or T&E strategy should articulate the cyber test strategy, including how the program manager’s organization will implement cyber DT&E guidance, and document the allocation of adequate resources to evaluate the system and inform decision making. The cyber T&E strategy provides the cyber-specific portions of the T&E strategy for the organization, and the CyWG

tailors and refines the strategy to meet the system development or sustainment needs. The cyber T&E strategy should summarize the cyber test requirements that the system developer should perform and the approach for assessing system developer tests, data, results, and remediation and mitigation implementation. The CyWG should ensure that all stakeholders have visibility into the agreed-upon plan for an adequate system evaluation, including the supporting data, testing, and required resources.

The TEMP or T&E strategy should:

- Describe the planned cyber test events, planned sequence of events, and specify which organization will conduct each test event.
- Identify the required data and tools.
- Describe the process for managing cyber vulnerabilities throughout the acquisition life cycle in the existing deficiency management program.
- Document plans for regression testing to reveal any newly introduced vulnerabilities, default configuration impacts, and other complexities potentially resulting from updates.

IDSK

The TEMP or T&E strategy will include an IDSK, which maps decisions and corresponding capability questions to operational and technical metrics and outlines data sources to inform the evaluation and decisions. The CyWG should identify all applicable cyber T&E data required to support the decisions in the IDSK. For more information on the IDSK, see Section K.2.7.

- Describe the VV&A plan and process for models, simulations, digital twins, and associated tools.
- Capture the funding responsibilities to accomplish cyber T&E, including available cyber resources and known cyber resource gaps. The cyber T&E resources should align with the T&E budget, which includes the funding and workforce for test conduct and support.
- Identify cyber T&E resources provided by the system developer in either the development or production contract proposals (see Appendix I:).
- Describe the personnel resources needed to support the cyber T&E strategy in terms of objectives specific enough to enable system developers to scope and cost out the testing with confidence. Include the CyWG members and personnel required for cyber analysis, testing, and assessments (see Appendix A:).
- Document the cyber test team members, including the test agency representatives; test observers; lab operators; vulnerability scanning teams; penetration test teams; threat stimulus teams; data collection and analysis SMEs; trusted agents; and system

administrators, defenders (including cybersecurity service providers (CSSPs)), maintainers, and operators.

- Include low-supply but high-demand physical assets such as labs, facilities, test assets, and operational platforms.
- Document the test environments such as labs, cyber ranges, representative interfaces, and networks, including mission-relevant, operationally representative, and/or actual operational networks and supporting systems. Include the limitations, either technical or administrative (see Appendix J:).
- Include the resources to complete VV&A of labs, cyber ranges, and M&S used for cyber T&E.
- Describe the representative threat capabilities (e.g., software or hardware systems).
- Document the tools and equipment necessary for conducting cyber T&E, for example, models and simulations, digital twins, specialized instrumentation for data collection and analysis tools, and testing and assessment tools.

See Appendix K: for a detailed outline of cyber DT&E–specific T&E strategy considerations.

3.5.1 Task: Synchronize Content with the Cybersecurity Strategy

Cybersecurity Strategy

A CSS should summarize the cyber T&E management approach, cyber T&E technical approach, and cyber T&E implementation progress. The CSS should not restate the level of detail in the TEMP or other T&E strategy.

The cyber T&E management approach should highlight the CyWG and summarize the cyber T&E organizations and other stakeholders supporting the chartered CyWG. The approach should provide the locations and instructions for requesting access to the data repositories containing all current cyber T&E information. The cyber T&E management content should summarize how the organization tracks, prioritizes, and verifies correction of deficiencies, vulnerabilities, and risks. Lastly, the management approach should summarize the cyber DT&E planning efforts and cyber DT&E process tailoring; depict the high-level cyber T&E schedule; and briefly address the processes to ensure that cyber T&E results inform DoW RMF assessments and all authorization decisions in accordance with DoWM 5000.103.



The cyber T&E technical approach should summarize the plans to conduct cyber T&E including system developer, government acceptance, government developmental and operational, and planned developmental and operational sustainment cyber T&E.

The cyber T&E implementation progress is the most dynamic element of the CSS once cyber testing of any type begins. The organization should always synchronize the CSS updates with the continuum of cyber T&E updates. However, updating and refining a CSS, and obtaining approvals, to remain current with the latest testing may be difficult. One approach could be to provide a link (in both the CSS and TEMP or T&E strategy) to a digital dashboard depicting the current cyber T&E status with links to detailed results. This approach enables all authorized stakeholders to have on-demand access to the status, test results, and assessments. Another approach is to use a collaborative document management tool that the organization routinely updates as cyber T&E implementation progresses.

3.5.2 Task: Refine and Update the Cyber DT&E Strategy

The CyWG should continually review information to understand the development of the system in terms of mission requirements, cybersecurity standards, and cyber resilience. The CyWG should review and assess MBCRA results and the existing test results to date before planning subsequent test events. As discussed in Section 3.3.6, usually a body of test results is available either directly from the previous activities and tasks or from sufficiently similar systems or subsystems. When choosing the measures, method of test, or data collection instrument, previous test results should inform the CyWG and test team choices. The case of "no prior test" is usually the exception. The CyWG should be aware of both the previous test results and the underlying data and context and may choose to prioritize upcoming events or methods based on the past results.

The CyWG will need to decide whether to use individual test plans to document data collection and analysis or use a separate stand-alone data management plan because of complex or detailed collection needs. Collection of good data (repeatable and relevant) is the fundamental point of conducting tests. The eventual test reports should provide data-substantiated evaluations and verification of system functional and nonfunctional requirements. Much of the substantiation comes from information captured during the conduct of the test. See Section 7 for test report information.

The CyWG should also consider whether shorter, quicker cyber test events early in development require formal test plans or if a digital living test plan approach can drive agility. In assessing T&E efforts, establishing processes, and refining the cyber DT&E strategy, the CyWG should always focus on and be able to answer the following questions:

- What system properties require verification?
- What is the depth and extent of evidence that would adequately substantiate an assertion one way or the other?
- What is the best way to collect the data required?
- How will the T&E events handle unknown or incomplete knowledge?
- How will the events handle data collections that will adversely impact the SUT?

Example: Refining Test Focus

A mission kill requires targeting a particular system through a narrow pathway. The CyWG might use a prior test result demonstrating the access path as a launchpad for additional testing. The CyWG alternatively may decide not to pursue a branch of testing because sufficient causal evidence in the cyber effects chain indicates effective mitigations. The CyWG may refocus test resources to try to find another way to achieve the same cyber effect (guided by the MBCRA and supporting documentation).

3.6 Artifact Generation

The iterative planning activities and tasks generate artifacts that the CyWG refines and references throughout the system life cycle. The CyWG should deliver, store, and manage the artifacts in the data repositories accessible to all authorized stakeholders at the proper classification levels. (Section 2.2.3 has additional information on data management, data sharing, and data repositories.)

4 Preparing for Cyber DT&E

The objective of *Preparing for Cyber DT&E* is for the executing DT&E organization (system developer or government) to complete the following activities:

- Gather detailed, tactical information for the cyber DT&E plan.
- Develop the detailed test plan.
- Prepare for and coordinate the test events identified in the individual test plans.
- Prepare for and complete DT&E readiness reviews.

This section provides insights into key activities and tasks as to how to execute these items.

In parallel with government T&E preparations, system developers will be completing preparation activities. During this time, the system developer will ensure that systems are meeting the stated developmental pace within the organization and communicating with the CyWG and test teams about the cyber test plans. Representatives from the CyWG or test team may want to:

- Witness system developer or acceptance testing.
- Clarify or adjust requirements so the developer can better scope and cost out the work.

If the CyWG has identified integrated or concurrent cyber testing in the strategy, then the CyWG should work closely with the system developer, government cyber test teams, and system performance test teams during *Preparing for Cyber DT&E* to meet multiple independent objectives without compromising the test objectives of any organization participating in the test.

Cadence Considerations

Cyber T&E timeline considerations align with the program's integrated master test schedule, system maturation timeline, acquisition pathway, development strategy, and deployment strategy.

Establishing timelines requires the CyWG to identify considerations such as what to test, what is available for test, what will the test inform, and what specific resources are available to complete each test event. These considerations will shape the scope and timing of each test event.

4.1 Inputs

The primary inputs for *Preparing for Cyber DT&E* ideally include:

- Cyber performance requirements and requirements traceability verification documentation.
- Information on the system design, mission, and mission-relevant environment.

- DoW RMF (i.e., DoDI 8510.01) artifacts, leveraged as needed:
  - Service-level agreements (SLAs) or active cyber defense agreements.
  - Organizational risk planning.
  - System categorization.
  - Establishment of a control baseline.
- Applicable SCG.
- MBCRA artifacts and results.
- PPP and CPI analysis and test results. CPI resident on the system may need AT protections, and if so, an appropriate agency will perform tests to verify AT protections.
- Criticality analysis.
- Available threat assessments.
- ICT supply chain illumination and risk analysis data.
- Hardware bill of materials (HBOM) and software bill of materials (SBOM) analysis.
- Attack surface characterization.
- Cyber portion of the IDSK. See Section K.2.7.
- Updated TEMP or T&E strategy.
- Test results from a current effort or similar system:
  - System developer DT&E activities (prototypes, subcomponents, integration testing).
  - System developer Service- or Component-level testing—testing the integration of components.
  - System developer full-system testing.
- Verification of fixes (VoF) reports.
- Software test plan or software assurance test results.
- Hardware assurance test results.

ICT Supply Chain

NOTE: "Supply chain" requirements for system developers include "cyber supply chain" or "ICT supply chain."

Traditional SCRM activities (i.e., making sure the right things are at the right place at the right time) may not adequately address cyber supply chain risks or concerns.

The Cybersecurity and Infrastructure Agency's ICT Supply Chain resource Library at https://www.cisa.gov/ict-supply-chain-resource-library provides additional resources and information

Also see Appendix F:.

This list is representative but not all-inclusive; individual programs may require other inputs as well.

4.2 Activity: Gather Detailed Cyber DT&E Plan Information

During preparation, test teams gather existing artifacts and data from the repositories. The CyWG and the specific executing test team make decisions about what to test, who will test, how to test, test boundaries, test measures (objectives), the schedule, where to test, data collection, data and asset classification, and reporting. The test team will document this information in the draft test plan (discussed in Section 4.3).

The primary determinant of a successful cyber test is a thorough and well-coordinated test plan. Test teams should ensure tight coupling of their test plans with the SUT requirements that the test plan intends to verify. Cyber DT&E focuses on verifying the effectiveness and technical implementation of the SUT's inherited and specified cyber requirements. When the SUT is the fully developed system, acceptance cyber T&E verifies and evaluates the specified requirements for system capabilities to prevent; detect; contain, mitigate, or eliminate; and recover from the loss of mission- or safety-critical functions in the required mission timelines before proceeding into government DT&E. Government DT&E also informs the system's readiness for OT in terms of safety and performance. The aggregate cyber DT&E events enable the understanding of the system's cyber behaviors and properties when exposing the system to a fully relevant environment later in the life cycle.

Both government and nongovernment test teams execute a test-fix-test process to discover and remediate requirement failures. The goal still is to develop valid knowledge of the SUT (and reduce risk for the follow-on development or government acceptance).

DoWM 5000.103 enumerates 14 requisite items when developing cyber DT&E plans. Test planning should center on mission-based scenarios, even by system developers. Approaches such as MBSE can help test planners craft mission-based scenarios to design effective mission-based testing by modeling and linking mission functions and supporting subsystems and systems. (Section 8 provides more cyber DT&E process challenges and DE considerations.)

As the test team develops the test plan, every decision will have a cost, risk, and schedule impact, which the test should determine and document. STAT methods (and personnel) can help identify the optimal set of test points and approaches depending on the character of the requirements and their associated measures (qualitative, continuous, or deterministic) (discussed in Section 2.4 which describes the role of STAT in cyber DT&E). Every test plan should develop the answer to the following questions (previously summarized in the cyber T&E strategy):

- Who will perform hands-on testing (system developer, lead government cyber DT&E organization, internal vulnerability test team, DCRT, etc.)?
- What is the SUT composed of (software, hardware, component, subsystem, etc.)?
- What are the objectives for testing this SUT?
- Where will the testing occur (range, labs, system developer facility, distributed, etc.)?
- What will the classification of the SUT, assets, and environment be *during* the test event?
- Why is the testing planned (controls assessment, architecture assessment, MBCRA verification, vulnerability assessment, etc.)? Refer to Table 2 in DoWM 5000.103.
- When will the testing events occur?
- How will the test team conduct the test (tools, infrastructure, resources, threat, etc.)?
- How will the execution of cyber test activities and events provide data for evaluations? What are the cyber test risks, limitations, and mitigations, and how are test results affected?
- What will the classification of the SUT, assets, environment, and test results be *after* the test event?
- Will the test team be able to remove system test assets and test tools from the test environment after the test event? Will the test team need to perform sanitization?
- How and when will the test team retest remediated or mitigated vulnerabilities to verify the removal of the vulnerability (e.g., during the event with system experts on hand, after the event)?
- How will the evaluations provide decision makers with essential information about the cybersecurity and cyber resilience of the system?

SMART

Individual components of the SMART (specific, measurable, achievable, relevant, and time-bound) framework synergistically combine to establish a thoroughly considered, distinctively defined, and measurably trackable target for test objectives. The WU SMART Goals Worksheet tool is available at: https://www.dau.edu/tools/smart-goals-worksheet.

When developing test plans, the test team members should ask themselves the following questions:

- Are the cyber performance requirements measurable and testable? Does traceability exist between each cyber requirement and a mission-critical/-essential task for the SUT?
- What types of metrics should the team consider for test cases?

- Was STAT considered when selecting the test points and sequencing?
- Does the team have the necessary tools? Do the tools have the proper authorizations (ATOs)? Can the team bring tools into/out of the test facilities? Can the team connect the tools to the test system assets?
- Does the team have the proper clearances, access, and permissions?
- Does the team have the right test environments (chambers, labs, traffic generators, etc.)? (Test environments are especially important for a SUT functioning as part of a kill chain, where requirements satisfaction may matter more to a downstream system than to the SUT.)
- Are the available test articles known and funded to perform as the SUT? (If the SUT is production representative, then the team should consider integrated test with OT.)
- Does the team have the right data collection means and methods?

When planning integrated cyber testing (see Section 1.6) or concurrent cyber testing (see Section 1.7), each individual organization (system developer, government test team, government test organization) should coordinate on specific test needs (e.g., system configuration, test objectives, test events, data collection) to ensure that multiple organizational perspectives and objectives are satisfied, if possible, without compromising the primary test objectives. The test teams should tailor cyber DT&E test plans to reflect the specific needs of concurrent and integrated tests.

Example: Unfunded Requirements

The CyWG may believe that a radar system is susceptible to a code-injection fault using a radio frequency pathway into the array face. The system developer asserts that this is not possible because the SUT implements a Harvard architecture for signal processing, based on the design specs provided to the subcontractor responsible for the subsystem. When the government requests proof (to verify by inspection that the implementation matches the documents), the developer states that there is no requirement to provide any documents beyond those on contract. This unfunded requirement situation results in additional costs and delays to satisfy the test team or increased additional risk and incomplete verification. The cost to add documents to the Contract Data Requirements Lists during the RFP is much less than the cost to modify the contract deliverables during development, and those costs are usually much less than the cost to redesign the radar array processing if the system fails the architecture requirement and inspection.

See Appendix I: for recommended contract language.

For concurrent cyber and non-cyber T&E test plans, the system developer, government test team, and government test organization may include the cyber T&E plan details as part of an overarching test plan (sometimes as an addendum) or as a stand-alone cyber test plan document.

For integrated tests, each participating organization (e.g., system developer, government test team, government test organization) will decide whether to participate in drafting an integrated test plan or drafting individual test plans describing the roles and test objectives for each organization's test event.

4.2.1 Task: Determine Contractual Basis and Pre-Work

Government test teams should work with program managers to reconfirm that a well-defined contractual basis exists to support cyber DT&E. Failure to do so (often claimed as a resourcing limitation) will result in test teams not investigating design risks while they are still manageable, leading to performing costly and time-consuming contract modifications. Included in this task is the government's responsibility to clearly articulate the requirements for system developer subcontractors. System developers should actively ask the government whether subcontractors are responsible for any flow-down requirements. Examples include:

- Visibility into the ICT supply chain granted to the government.
- System developer/subcontractor ICT SCRM.
- Software source code data rights (or rights to review source code and development or compile environments) granted to the government.
- System developer, subcontractor, or both support of test, evaluation, or analysis events such as TRRs.
- Right of execution or receipt of results of system developer/subcontractor execution of cyber testing of system development environments granted to the government.
- Access to system developer/subcontractor facilities granted to the government.
- System developer, subcontractor, or both participation in MBCRA events.
- Access to system documentation and SMEs granted to the government.

4.2.2 Task: Define the Test Type(s)

Table 2 in DoWM 5000.103 provides a comprehensive list of 26 types of tests that the test team can tailor appropriately for the SUT to collect the data. These types consider the range of perspectives, means, timelines, and targets of a cyber developmental test (DT). The term "tailor" describes the process of adjusting the test means and methods to satisfy the eventual goal and reduce extraneous effort not supportive of those goals.

Before design reviews, the CyWG may choose to perform an architectural vulnerability assessment, MBCRA iterations, or a resilience analysis. Conducting a vulnerability assessment to highlight structural risk areas will help reduce the chance of cyber failures and findings, regardless of subsequent hardware or software choices. As the system developer makes those design choices, the test team may decide to incorporate ICT supply chain testing (see Appendix F:), software and hardware assurance, or cloud testing (see Appendix H:). Once the system design is complete and undergoing verification, the test team might incorporate penetration testing, vulnerability assessment, STIG testing, or reverse engineering testing to verify the prevention of negative use cases. The CyWG should consider where the SUT is in its maturation and select test types that best answer the most pressing questions for the upcoming phase of maturation. Developers may contribute artifacts demonstrating AT, ICT SCRM, or mission assurance and cyber resilience design features for verification by inspection. M&S can be a powerful tool for rapid and wide-ranging cyber resilience and risk investigation, given that the M&S environment, articles, and behaviors are sufficiently consistent with the SUT as delivered. The test teams will need to decide the proportion of effort put into M&S with the required verification and validation (V&V) in conjunction with live testing on a real article.

Example: Naval Air Systems Command Cyber Test Series

CS 100 Performance Baseline
CS 200 Restoration
CS 300 Vulnerability Scans
CS 400 Code Alteration
CS 500 Exfiltration
CS 600 Geo fencing
CS 700 Awareness
CS 800 Penetration Test
CS 900 Counter Navigation
CS 1000 Denial of Service
CS 1100 Resilience

When deciding on the type of cyber DT&E tests for a given *Preparing for Cyber DT&E* activity, the CyWG or system developer should consider the opportunity or need to conduct integrated cyber testing (see Section 1.6) or concurrent cyber testing (see Section 1.7). The CyWG should refer to the IDSK (see Section K.2.7) and overarching cyber T&E strategy in the TEMP or T&E strategy for opportunities to conduct (1) integrated system developer and government cyber DT&E, (2) integrated government cyber DT and OT, and (3) concurrent cyber and non-cyber testing. The CyWG should work closely with each stakeholder to ensure that test events and data collection will satisfy each individual stakeholder's needs while maintaining independent evaluation, analysis, and reporting.

As the CyWG scopes the cyber DT&E activities and test types, they should consider and plan for test facilities to host test event execution. System developers can build their internal testing to mirror these test types and objectives and to conduct verification pre-release to the government. Table 4-1 lists example test facilities and assets, and test types that test teams may wish to use for cyber DT&E activities.

Table 4-1. Cyber DT&E Activities, Facilities, Assets, and Types

Cyber DT&E Activities	Test Facilities and Assets	Cyber Test Types
Verification of pre-implementation cyber factors (design, cyber supply chain risk management, etc.)	System developer, suppliers, and/or design-review analytical process	• Architectural vulnerability assessment • Mission based cyber risk assessment (MBCRA verification • System misuse and abuse testing • Information and communications technology supply chain testing • Critical infrastructure assessment
Component, software, and hardware unit/pre-integration and/or subsystem test	• System developer, government unit test environment, formal models • System software and hardware components/subcomponents	• Software assurance testing • Hardware assurance testing • Reverse engineering/anti-tamper evaluation • System misuse and abuse testing • Platform and component hardening verification • Software factory testing • Cloud testing • Non–Internet protocol device and component testing • Cyber-electromagnetic spectrum operations (EMSO) testing
System integration test or full-system test	• System integration facilities, lab-based digital twin representations, simulators, cyber ranges such as the National Cyber Range Complex nodes, shielded cyber/electronic warfare test facilities • Full system, system software, and hardware components/subcomponents	• Cyber functional verification vulnerability assessments • Cloud testing • Security Technical Implementation Guide testing • Control testing • Cyber-EMSO testing • Cyberspace kill chain testing • Interface testing • Network vulnerability assessment • Resilience testing • System misuse and abuse testing

Cyber DT&E Activities	Test Facilities and Assets	Cyber Test Types
Mission-relevant test	• Government hardware-in-the-loop facilities; cyber ranges with an approved verification, validation, and accreditation for the system under test; digital twins; spread benches; cloud environments (with host permission) • Full system, system software, and hardware components/subcomponents	• MBCRA verification • Concurrent cyber and non-cyber testing • Cyberspace kill chain testing • Cyber-EMSO testing • Penetration testing or exploitation analysis • Purple team testing • Recoverability testing or continuity of operations testing • System misuse and abuse testing • Incident response testing • Bug bounty (classified or unclassified) • Threat hunting

4.2.3 Task: Develop Cyber DT&E Test Objectives

When developing test objectives, test teams should study the system requirements, MBCRAs, CONOPS, or other documentation describing SUT performance in the designed environment. Test teams should consider the mission context when developing cyber DT&E objectives.

- Does the test team understand each of the following?
  - System behaviors.
  - Cyber performance requirements and criteria.
  - Anticipated operator workarounds.
  - Mission-critical functions.
  - Critical data.
- Are data collection and instrumentation positioned to capture the relevant data?
- Is the V&V complete or are the elements needed for integrated developmental and operational VV&A provided?

Test Conditions

Mission-relevant testing requires a production-representative SUT in an operationally representative or mission-relevant environment, but certain test points may require testing in more controlled conditions to ensure conclusive results. These conditions may include controlled stimuli, additional instrumentation, other data collection capability that is not present on mission-representative systems, or modification of AT controls to ensure that the test teams do not accidentally invoke the AT penalty application causing the SUT to no longer be usable (e.g., brick the system).

Table 4-2 lists example cyber DT&E test objectives. Test objectives inform cyber DT&E test plans and have a large role in setting the test environment needs.

Table 4-2. Example Test Objectives

Example Test Objectives	Example Technical Test Methods	Example Metrics
All code within the user authentication subfunction follows code-quality standards, and the code implements the approved state machine. Examples: • Verify that the developer is following the levied code-quality requirements, which specify: every "if" statement requires an "else" statement; a maximum number of source lines of code (SLOC) count; no external library calls; and boundary checking and enforcement on all inbound calls. • Verify by formal techniques that the approved state machine (code-agnostic instruction set) is complete and correct using the NIST SP 800-160 assurance case process.	• Verify with two independent code review tools that the delivered code compiles into an executable program. • Review precompiled code to verify the enforcement of state machine features and prohibitions. • Review precompiled code to ensure conformance with quality standard features. Compile code in a stand-alone machine with no libraries loaded; observe compile completed without failures; and run executable through sample mission profile to ensure functionality.	• Number of violations per 1,000 SLOC for code-quality standards (If/Else, SLOC count, libraries). • Number of boundary-check failures. • Enumeration of unplanned/undesired feature(s) in compiled executable due to quality violation. • Number of possible states that are noncompliant with the state machine in the delivered pseudocode.
Verify that the system under test (SUT) takes active measures to identify and deny unauthorized access attempts, including denial of service and distributed denial of service, at the system, its internal boundaries, and cross-domain interfaces with other systems.	Verify: • Access control denies access to unauthorized connections and user/process interactions. • SUT identifies and denies unauthorized attempts (within a specified performance threshold). Effectiveness of internal and external boundary defenses.	Percentage of tested malformed and invalid inputs blocked or dropped.
Verify that the SUT detects and discards malformed messages and invalid inputs.	Verify that the SUT validates data inputs for mission-related data.	Percentage of tested malformed and invalid inputs blocked/ dropped.

Example Test Objectives	Example Technical Test Methods	Example Metrics
Verify all data via cryptographic hash comparison before loading the data into the munition's operational memory for all data loads.	• Upload known-good data loads; ensure passing within mission timelines. • Upload known-bad loads; confirm rejection of bad/ malformed loads within threshold criteria timeframes. • Upload incomplete/ indeterminate loads; confirm rejection within acceptable timeline. • Stimulate logging functions; confirm logs are accurate and protected. • Examine the SUT relative to cryptographic device assumptions and ensure that the SUT adequately satisfies requirements and conditions.	• Total time to upload or reject. • Number of correct accept/reject actions over number of attempts. • Negative testing: Bad upload successful? (i.e., resulted in a malfunctioning weapon) – yes/no. • Entropy value of the hash. • Number of questionable or failed prerequisite conditions for crypto modules/ devices.
Verify that the SUT monitors the configuration baseline for cyber anomalies in real time by 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.	• Determine the SUT's susceptibility. • Examine the integrity and confidentiality of critical-mission data. • Ensure that cryptographic devices are operating as intended.	• Percentage of malicious code detected in tested software. • No unauthorized software is resident on the operational system.
Verify that the SUT recovers mission-critical functions to enable mission completion.	Verify that the SUT fully recovers required mission-critical functions.	SUT recovery falls within acceptable mission performance thresholds.
Verify that the SUT degrades gracefully (e.g., quality of service) before degrading to unacceptable mission consequences.	Verify that the SUT maintains the minimum performance required to prevent adverse mission consequences.	SUT degradation falls within acceptable mission performance thresholds.
Confirm digital signatures and system developer–approved techniques for authenticating software patches and updates.	Verify that the patch process authenticates all software patches and the system updates before initiating the patching process.	Percentage of software patches and system updates authenticated before patch initiation.

Example Test Objectives	Example Technical Test Methods	Example Metrics
Verify that the system's automated tools identify altered patches and software updates and that the altered patches and updates do not successfully authenticate on local or remote components.	Verify patch and vulnerability management effectiveness, including timelines for pending patches and critical patches.	Percentage of critical patches deployed within the required timeframe.

4.2.4 Task: Understand Commercial Infrastructure Interfaces

The test team should have visibility into the SUT and be able to define the scope of the test on the SUT. When testing a SUT that uses commercial infrastructure, such as telephony switchgear, Internet service provider routers, cloud services (see additional information in Section 4.2.5.1), or leased bandwidth (such as satellite or terrestrial data communication), the test team should understand the lines of demarcation and legal restrictions. Except in very special circumstances (clearly articulated before testing begins), the test team may not have the authority to test commercial infrastructure and should plan to mitigate potential risks during a test where the SUT connects to commercial infrastructure. In general, commercial data communication infrastructure is responsible for providing a circuit, and test teams generally have very little visibility into what the circuit carries, especially when using encryption technologies and techniques. The test team commonly assumes the existence of a failure in the commercial infrastructure and plans to contain the test effects within the SUT boundary. System developers will need to work with the CyWG to ensure that predelivery test assumptions are valid, and the government will need to think carefully about the cost implications of the worst-case stance. As the design matures, the system developer and CyWG should work together to highlight design areas of special sensitivity to compromise or malfunction and focus commercial security and assurance techniques on those areas.

Commercial Infrastructure

In addition to hardware or physical components, commercial infrastructure may include open-source libraries, microservices, or commercially hosted "as-a-service" capabilities.

Another possible use of commercial infrastructure is in DevSecOps, where an application may invoke libraries or microservices hosted by a commercial service at a particular runtime. If a software application is incorporating software from a nongovernment or "open" source, the test team should identify and test the software as a commercial service. In the case of open-source libraries and microservices, the CyWG should seek explicit requirements about security and functionality enabling verification.

Finally, in certain structures (such as the acquisition of services), the program manager's organization may import a commercially hosted "something"-as-a-service (e.g., software as a

service (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS)) capability. The government may have very little leverage or ability to enforce cyber requirements on the commercial company or to conduct an MBCRA within the system developer's boundary. In this case, the CyWG will want to work with the system developer to obtain as much information as possible. The CyWG should also build a framework for what is or is not known about the service and prioritize participation in the MBCRA risk process to inform all stakeholders about mission risks. The CyWG will also want to leverage information from other government entities using the commercially hosted capability and share test results and strengths/weaknesses. Platforms that use, or connect to, a system or service (such as commercial systems) with an unknown cybersecurity status should assume compromise of the connected system or service until and unless it can be proven/accredited trustworthy (a true zero-trust assumption).

Appendix J: contains additional considerations on cyber DT&E test infrastructure and environment planning.

4.2.5 Task: Document Unique Considerations for Specialized Assets and Techniques

Increasingly, the focus of cyber DT&E efforts includes specialized assets, specifically:

- Unique technologies and hardware components, such as cloud-based environments, radio frequency (RF) spectrum considerations, space and other autonomous vehicles, or non–Internet protocol (IP) communications.
- Specialized tools, such as traffic generators and fuzzers, MBSE tools, or cyber-over-RF tools.

Test Considerations for Specialized Systems

Request the CUI Appendix L, "Cyber DT&E of Specialized Assets," from Appendix L (CAC) for additional guidance.

Tests involving these considerations may demand unique expertise from the test team to ensure that test plans address the considerations related to these factors.

Be Aware!

Testing intricacies might exist at other security levels for several types of non-IP based systems and require additional considerations for cyber DT&E. Plan these scenarios in advance so as not to be caught off guard during test execution, which could risk test results as well as test assets.

4.2.5.1 Technologies and Components

Artificial Intelligence (AI). Test teams will need to navigate two issues: (1) AI-enabled capabilities and systems and (2) AI tools used to execute tests.

Test Considerations for AI-Enabled Systems

The Digital Appendix M, "Cyber DT&E for AI-Enabled Systems" (which is under development) has additional AI cyber DT&E guidance. The content is available upon request from Appendix M.

- **AI as the SUT**. System developers are beginning to employ AI-enabled capabilities for certain limited uses within DoW systems. Test teams should understand the relationship between the stated mission and conditions versus the machine learning training set and layers or weights within the AI system. When testing AI systems, the mission and context should be well-defined (internally consistent, traceable, and sufficient to the mission environment). See Appendix M for additional guidance.

- **AI as a test tool**. When considering whether to use AI as a test tool or an AI-enabled test tool, test teams should ensure that any results obtained using AI as a test tool to test a SUT are explainable and repeatable. Otherwise, the AI may produce hallucinations or mistakes, and these will make the test results irrelevant.

Commercial services. Where the SUT uses a commercial service provider, contractual restrictions may limit cyber DT&E. In place of direct T&E, the CyWG should seek attestations or test results from internal testing. Test teams may need to find additional expertise to evaluate these systems or receive results from the service provider. In addition, if the test plan indicates to "over-the-shoulder" observe the cloud provider test, the plan should delineate the required expertise of the test team members to be present during the event.

Cloud. Cloud technology is similar but not identical to commercial infrastructure in potential limitations of authority. Cloud technologies operate in some way like a legacy mainframe, sharing memory and execution space between distant user interfaces. Modern systems can be very complicated to test because of dependence on the management and control applications that may have layers of privileges and configurations, each with mission

Test Considerations for Cloud Environments

Mission owners deploying systems into cloud environments may be using Agile development methods or employing DevSecOps to develop and deploy software. Appendix H: and the DoD Software DT&E in DevSecOps Guidebook contains additional information (https://www.cto.mil/dtea/software/).

The Cloud Computing Security Requirements Guide (https://public.cyber.mil/dccs/dccs-documents/) has additional information on testing in cloud environments.

impact. The CyWG should request explicit information from cloud providers (government or commercial) about the invoked functions and services at each functional layer. Composability of security claims across a cloud fabric will be a necessary test team skill.

Composability

Cloud implementations may base their security on assertions made by other external service or application providers. The overall security of the system is composed of the interaction between the elements. The system is considered "composable" if its overall security is maintained when combined with a group of security assertions. If the SUT intends to make assertions about security being a composable feature of the system or intends to base its security on the claims of an external entity, the test team will need to have the skills required to evaluate these composable security claims.

Formal Methods/Formal Assertions. A strong design principle for reducing cyber risk is to invest in the fundamental development environment itself. Techniques include formal methods verification, verifiable compilers, trusted operating systems, and the use of strongly typed, memory-safe programming languages.

Example: Cyber DT&E of Heterogeneous Fault-Tolerant Architectures

In the development of complex systems, particularly those operating in challenging environments like space, system developers may employ specialized architectures to ensure resilience and reliability. One such architecture is the heterogeneous fault-tolerant architecture (HFTA). HFTA is a design principle using diverse components and systems to achieve redundancy, reducing the risk of common mode failures and making the system resilient to both accidents and adversarial threats.

This approach is particularly useful in environments where random faults, such as those caused by radiation in space, can occur. By using different manufacturers, operating systems, and software, HFTAs can minimize the risk of a single fault causing a mission kill. HFTAs also offer significant cyber resilience benefits because there is no single path kill chain for an adversary to exploit.

Implementing an HFTA, however, often requires increased size, weight, power, and cost and increases the supply chain footprint. The CyWG should be aware that if the system developer uses partially implemented HFTAs, it could still allow certain common-mode threats or failures. For example, using three different manufacturers but sharing the same compiler libraries to build executables can create a partial HFTA with limited resilience. The risk of a common compiler compromise should be either accepted or mitigated another way.

When testing an HFTA, cyber DT&E teams should recognize the architecture's inherent resilience and adjust their test plans accordingly. An MBCRA with expanded criticality analysis should help identify areas of redundancy and potential vulnerabilities. Test teams may want to focus on possible vulnerabilities in partial HFTA designs, where common modes can still exist.

Testing an HFTA requires a detailed approach because the architecture is meant to withstand faults and exploits. Test teams may not be familiar with declaring resilience even in the face of a possible exploit, as the HFTA's diversity and redundancy make it difficult for a single exploit to cause a mission kill. By understanding the HFTA's design principles and limitations, test teams can develop effective test plans and avoid wasting limited time and resources on traditional test techniques.

Many formal specification languages and implementations meet these criteria, such as RISC-V, seL4, the National Security Agency (NSA) distribution of Solaris with Trusted Extensions, TLA+, Integrity, CompCert, Java, and Rust.

When leveraging these formal and safe implementations, developers may provide attestations or assurance cases based on formal methods, for example, some systems utilize the TLA+ foundation for critical components. In the code itself, developers may assert the "unreachability" of a particular undesired state. This shift towards formal verification requires the test team to acquire additional expertise to evaluate the strength of these assurance cases and formal-methods constructions. It is important to remember that assurance cases are typically based on a specific set of assumptions and constraints, and the scope of the security assertion is tightly bound to those conditions.

Physically remote SUT. Certain systems are built with extra resilience features or increased autonomy to handle austere or disconnected environments. These include unmanned underwater vehicles (UUVs) and spacecraft, for example. Certain spacecraft may allow one subsystem to reboot another. Both UUVs and spacecraft might be able to accept a completely new operating software load via remote means, and test teams will need to conduct testing without the physical asset returning to a lab.

4.2.5.2 Specialized Tools and Design Techniques

Many system developers are using model-based and digital design, which will likely change the cyber DT&E plans for the system. Certain development tools, such as MATLAB, Scriptcase, or PathMATE, either generate or convert executable code based on a set of targets and inputs versus software engineers coding by hand or from a library. Even in this environment, the system will have security properties expressed in the pseudocode or MBSE model structure—these will take the case of security targets and assertions against those targets. Developers should still generate the evidence that evaluators will need to verify the cyber requirements. Cyber test teams should examine and evaluate the security properties of the inputs and compilers, interpreters, libraries, or all, that build the executables. In the case of automatic code generation, the test team should verify that the executable output faithfully executes the mission and safety functions when developers and engineers document the design. For model-ingestion tools, examine the MBSE model input that the code-generation tools are using. In both cases, the T&E question will be whether the output software satisfies its cyber requirements.

The three most common MBSE modeling languages for DoW systems—DoDAF, UAF Modeling Language, and Systems Modeling Language (SysML)—do not currently document cyber in a way considered to be complete and detailed enough to enable analysis and T&E. The Risk Analysis and Assessment Modeling Language (an extension to SysML) is an improvement

but not yet widely fielded. Test teams unfamiliar with MBSE approaches and tools should seek specialized training. If the development environment uses these digital techniques, the test plans should include how to evaluate the environment. (Section 8.5.1 discusses MBSE in more depth).

Example: Complex Testing Scenario

Systems with low connectivity, such as long-duration UUVs or some spacecraft, should undergo rigorous testing before installation and deployment. The launch and test teams should work together to ensure that cyber testing and environmental testing are working together.

Most spacecraft launches will initially be in a holding orbit for testing and checkout before boosting to an operational position once checkout is complete. In this case, the CyWG should plan to complete most tests before the prelaunch prep sequence and should plan for an additional on-orbit test period, including the security implications of software updates or modifications to an on-orbit system. For most satellites on orbit, there may only be a narrow window to transmit/receive, or the test team will need to rely on relays (terrestrial or space).

UUVs may stay local for testing and checkout before going into the open ocean. These systems may need to transit or break off from a mission to establish direct or relay connectivity, and test teams will need to plan for the unique T&E factors associated with systems that have limited or intermittent connectivity, such as UUVs and spacecraft.

4.3 Activity: Develop the Test Plan

Cyber DT&E test plan content and depth depends on the type and intent of the test; SUT; test objectives; planned testing activities; resource agreements; agreed-upon assumptions; common test scenarios; operational mission impact context; desired outcomes; and data collection, management, and analysis requirements. Table 3 of DoWM 5000.103 provides a common set of test plan data for consideration when identifying the test plan content needs. It also offers a template for how to group test plan content into test plan document sections. Contractor system developers might not be bound to DoWM 5000.103 when they are not satisfying a Contract Data Requirements List (CDRL) and may choose to follow internal guidance and policy when developing contractor test plans. Table 4-3 expands on the information in Table 3 of DoWM 5000.103 and provides an example test plan outline with specific considerations and details suggested for each section. Data Item Description (DID) DI-MGMT-82140, "Naval Aviation Cybersecurity Test Plan," contains a listing of test plan items, as an additional reference.

Reminder

Because people move to new jobs or because of other variables, the test team who planned the test and the team who performs the test might have different members. It is important to write a test plan that is understandable to anyone executing the test and generating the report.

Table 4-3. Example Test Plan Outline

Topic Heading	Amplifying Information
Test Overview and Foundation • Summarize the test objectives and measures. • Provide a SUT description. • Identify the external connections to the system and which external interfaces the test team expects to include during the test. • Describe the system's supply and sustainment chain if included and how the test team plans to assess the information and communication technology (ICT) supply chain components.	**Objectives and Measures**: The fundamental objective of cyber DT&E is to verify requirements and to document residual risk. Test teams should ensure that every test objective is valid within the mission-relevant context and is traceable to an explicit or implied system requirement; test teams should document the trace in the test plans. The test team should ensure they have documented and derived measures for each test objective before the test. Scientific techniques can assist with understanding test points measured in terms of continuous variables (like time) or binary responses (as in the decision to deny or permit). Judge qualitative measures (e.g., the strength of procedural controls against supply-chain compromise) as evidentiary cases, not numerical, and rely on the test team's and evaluators' documented judgment and experience. **SUT**: The SUT should usefully represent the system to which the requirements apply. The test team can use a development instance; a production asset; or some collection of models, simulation labs, or test stand-ins specifically procured for the purpose. In each case, the test team will need to describe the validity, risk reductions, and what-if cases (e.g., what happens if the asset is accidentally damaged). For real-world test articles, expect more emphasis on risk reduction, safety, etc. For the inverse (heavy modeling and simulation cases, prototypes, emulation, etc.), expect more emphasis on verification, validation, and accreditation. **External connections and ICT Supply Chain**: There are several ways that pollution of external dataflows can occur: either timeliness (too early, too late, out of sequence, wrong time); intelligibility (too many bits, too few bits, out-of-sequence bits, garbled headers); or veracity concerns (receiver wrongly trusts transmission). However, not every dataflow pollution affects the parent process or overall mission. Where it is relevant to test by manipulating external interfaces, the plan should note which ones, how, and why. For the ICT supply chain, components (not just hardware but software including microservices and compilers) may be suspect, counterfeit, compromised, or unreliable (among other problems), but again, test teams should know the system and mission impact of different dataflow concerns and, in the plan, should specifically document the relevance to the test.
Management of the Test • Document the roles and responsibilities—both operational roles and assessment roles. • List the entrance criteria for the test.	**Running the Test**: Choose T&E timing to help drive decision points in the system life cycle informed by the Integrated Decision Support Key (see Section K.2.7). Measures, scoring, and retesting: In greater detail than in the measures summary, the test plan should cover the scoring and sufficiency for cyber findings, so the test teams know

Topic Heading	Amplifying Information
• Summarize the schedule, events, and locations. • Document the test requirements and required resources (including risks and mitigations): – Test articles. – Funding. – Personnel. – On-site space, secure storage needs, and accommodations. – Connectivity and network connections. – Special training requirements. – Test limitations and special cases. – Authorities (e.g., authorizations to operate or connect) and approvals (e.g., visit requests).	when they have collected enough of the right data to meet the objectives. **Time and Resources**: The test plan (or equivalent) articulates the schedule and resourcing decisions made in the previous steps. The test plan also covers risks to the test, risk mitigations, and test limitations. The resources section includes funding, range time, time with the test article, test personnel, specific tooling and/or data collection instrumentation required, exploit development, SUT availability, SUT maturity, and software licenses (if required). Cyber DT&E often requires unique tooling to stimulate SUTs and capture SUT responses. Stimulation and data collection mechanisms should be authorized to connect to the test environment. The plan should document the risk reductions and test limitations if it is informing a test readiness review.
Execution Details • Scope the assessment: Refine the major activities of the test strategy and how testing will flow to meet the test objectives. • List the required documentation and artifacts assessment. • Describe: – Technical controls assessment. – Attestation to verify the existing software conditions before, during, and after conducting test methods. – Sanitization methods for how the test team will clear test data and effects. Is the test team able to remove all equipment (e.g., test tools and test assets) from the test environment or are there contamination or spillage concerns? • Describe methodology and approach: – Cyber threat representation. – Data handling, including security classification guides (SCGs). – Event preparation. – System operation and required users.	**Test Environment:** The T&E team should describe the test environment, specifically the larger context of the test. Also important are the assumptions, limitations, and constraints placed on the test, especially those that might affect the validity of the results. The system does not need to be in its operational environment (but a mission-relevant environment could support integrated DT/OT). The SUT may experience failures, and the test may expose environments to risks from accidents, unintentional misuse or misconfigurations, and cyber threats. Test teams may choose to prioritize field trouble tickets and intel threat reporting when choosing the test event order but should not limit them to only those potential malfunction and cyber event cases. **Fix Verification and Retesting**: Cyber DT&E should use a test-fix-test approach to close results and deficiencies identified during current or previous testing, providing evidence of remediations. The fix may need retesting to satisfy the requirement or close the deficiency report (DR). Test teams should be cautious to offer mitigations for DRs unless they are explicitly tasked to do so. If so, test teams should be vigilant and rigorous about maintaining independence and effectiveness in fix verification. **Choosing What and How to Test**: Mission based cyber risk assessments (MBCRAs) should identify potential vulnerabilities and attack scenarios ahead of the test and should be a source document for the test plan. MBCRAs will estimate the mission impact to allow the prioritization of findings, deficiencies, etc. For those SUTs with requirements to withstand a particular offensive attack or challenge, the test plan should cover the validation of the points and the test tools that replicate them as faithful representations of the

Topic Heading	Amplifying Information
– Vulnerability assessment, penetration testing. – Specialized assets (e.g., non-Internet protocol–based, embedded system testing). See the CUI Appendix L. – Possible instrumentation (e.g., special tools used to collect radio frequency signals or other data processing information). – Mitigation plan: Describe the plan to fix and retest prior or newly identified vulnerabilities. – Deviations: limits, authorities, and procedures. – Assessment tools. – Tools for testing black-box technologies, as required. – ICT supply chain assessment techniques (see Appendix F:).	attack or challenge. There may be complicated classification issues to work through with certain adversary emulation techniques. Certain Federal labs can assist test teams with analysis (to guide targets/how to test), and threat-representative attack tools can expose a system to a host of varied techniques. These techniques can verify both active and passive defensive regimes, depending on the information flow of the SUT.
SUT Specifics • Document the system configuration under test, including software and hardware component versions. • Describe the cyber test techniques used for the assessment that are specific to the SUT: – Operational SUTs. – Maintenance ports. – Network testing. – Embedded system testing. – Software testing.	**Self-Protective Capabilities**: Proactive defensive or assurance design and function allocation is structurally focused or “baked in” to the system design. Test teams should validate the assertion of the SUT implementation to the secure design and may require a more evaluation-heavy focus of effort. “Reactive” defenses seek to detect and respond to potential problems. Where the SUT has a funded and allocated “cyber defense” (such as a U.S. Air Force mission defense team or a Defense Information Systems Agency cybersecurity service provider), the test plan defines those capabilities as either in or out of scope for the test article, depending on the allocation of requirements to external entities. In some cases, the defensive entity may allow the test to use a representative capability to verify the requirements through testing. These defensive capabilities are the “bolted on” variety. NOTE: The proxy defensive capabilities/personnel, if existing/present, should be representative of actual, contractual, defensive capabilities deployed with the system when fielded; there should never be defenders present just for a test.

Topic Heading	Amplifying Information
Data Collection Plan • Describe the data collection tools. • Describe how the data contribute to demonstrating the requirement or test objective. • Discuss how to store, index, and retrieve data using data security best practices. • Describe the tools that ingest and process/analyze data to allow the test team to develop and defend insights about cyber requirements. • Address the classification in accordance with the SCG, any applicable horizontal guides, classification by compilation, and proprietary information concerns. • Document any test deviations and impacts on data collection.	**Data Collection**: Data collection is essential for documenting results, assisting developers with fixing DRs, and reducing risk. Data collection may be a section of a test plan or a stand-alone data collection plan. Classification of collected data may be based immediately on the SCG or may require analysis of the compilation of detailed system performance; and data may include proprietary elements. **Vulnerability ID, Documentation, and Tracking**: When storing DRs in a data repository, each documented deficiency should have a unique tracking ID for the discovery and retrieval of data. The test plan should discuss where and how the program will track and assign each deficiency. Having system documentation available to provide the details on DRs will help the engineers and the system developer devise mitigations in response to the report, not just for a particular instance of a finding but for classes of vulnerability.
References, List of Symbols, Abbreviations, and Acronyms	As required.

4.4 Activity: Prepare for Cyber DT&E Events

Preparing for Cyber DT&E events happens continuously and on parallel timescales, but it is primarily a people-driven endeavor, aided (but not governed) by technology.

Cyber T&E Tools, Facilities, and Service Providers

To search for and learn about cyber T&E supporting tools, facilities, and service providers go to https://jetep.apps.dso.mil/cyber_te.

For more information, contact OSDRE-DTEA-Cyber@groups.mail.mil.

Test Organizations. Each test team should develop and maintain a contact list for activities with the internal and external organizations that the team works with to prepare for test events. This list will be useful when finding and reviewing prior test reports; confirming funding, staffing, and resourcing; prepping and emplacing data collection or test instrumentation; and conducting confirmation reviews of security classification guidance. The Joint Engineering and Test Enterprise Portal (JETEP) maintains a list of capabilities and test entities (Centralized Cyber Capabilities Directory) for test team discovery and coordination. System developers use corporate practices and participation in industry and government forums and employ a variety of methods ranging from internal red teams to third-party expertise, to rental of

government cyber range facilities, and variations in between as appropriate for the SUT and the test.

Scoping. Especially for complex SUTs, such as cloud or containerized systems, test teams should invest extra effort to be clear on the target of the test (e.g., what to stimulate, boundaries, in-bounds, whitelists, out-of-bounds, blacklists); the method of test (how to stimulate); the path to get to the injection point; and the potential outcomes. (Further details are available in Appendix H:.)

Example: Assumed Starting Conditions

- ✓ Assume the system's information was exfiltrated.
- ✓ Assume there will be hostile physical access to the system.
- ✓ Know the system and the mission- and safety-critical functions.
- ✓ Pay attention to how to operate.
- ✓ Focus on detection.
- ✓ Plan the system recovery.

Asset and Range Coordination. The cyber DT&E test team should coordinate with cyber test facilities and ranges and with the owner of the test article(s). Test articles may be live systems, models, constructed environments, dedicated test assets, bench setups, etc. For certain systems, test teams may need distributed assets or facilities with distributed connectivity. Teams may need to ensure security segregation of tools from assets, data collection, or both. In other cases, the test team may need to ratify the permission and access for a team to test a certain system (e.g., ATO, ATC). The test team may need to coordinate agreements, such as a memorandum of agreement (MOA), memorandum of understanding, or other documented agreement, or may only need to coordinate by email or meetings. The program manager's organization may assist with these agreements or execute these on behalf of the test team, if needed.

If not already considered by the CyWG, relevant additional inputs for consideration include:

- The capabilities and limitations of the various test tools and ranges.
- The capabilities, limitations, and limits of certification of the test team itself, specifically the authorized cooperative and adversarial techniques in use.
- The limitations and prerequisites of the data collection and data processing tools.
- Any validation or risk-reduction events executed before testing, including attaining interim authorizations to test or other necessary certifications.
- Prior test results, T&E results from similar platforms or common subsystems, and VoF results.

NOTE: The test team should document any of the above considerations in the test plan.

Over time, cyber DT&E teams will often develop and maintain the experience and expertise to constitute the teams with focus areas such as specific mission areas, data processing environments, testing/exploitation tools, or communication protocols. The teams may invest in

skills-exchange personnel arrangements or participate in trade events to increase the awareness of their mission or maintain the cutting edge of tools and capabilities. While just-in-time training may be possible for very specific needs, it is generally not a reliable or preferred approach. The JETEP Website, depicted in Figure 4-1, may also be a resource for setting up skill-share or personnel-shadowing arrangements.

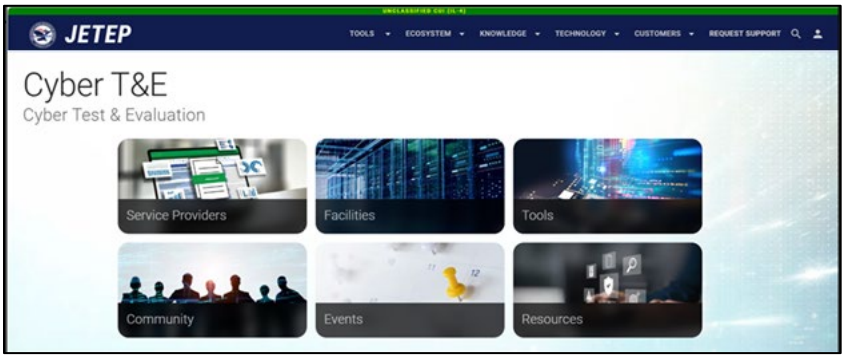


Figure 4-1. JETEP Website

4.5 Activity: Conduct Cyber DT&E Readiness Reviews

For most organizations, the TRR is the final approval with authority to indicate that the test is ready to proceed. System developers likely follow internal guidance and policy for a readiness review when developing test plans. The program manager's organization can request system developer documentation for readiness reviews as part of the contract. System developers will also conduct internal reviews to ensure their specific components, modules, or subsystems are ready for government integration testing or system-level testing. TRRs may have a variety of entrance criteria including:

- A signed test plan (or commensurate document).
- Approved ATO or interim authorization to test (as required).
- SUT schedule and availability confirmed.
- Confirmed test team access to the SUT.
- Satisfaction of other prerequisites as defined by the test plan.

Barring other guidance, a TRR should include a review of:

- Test objective/requirements for verification.
- Measures and metrics for the assessment of requirement satisfaction.
- Rules of engagement (ROE) for the test team (e.g., Is it acceptable to plant flags or trigger real effects or will planting flags trigger unrecoverable real effects?).

- Limitations and risk mitigation/safety for the test team, SUT, and test environment (e.g., including in or on cloud assets, embedded systems, avionics components, munitions).
- Test team's plan to monitor for test escapes and response options.
- Testing required for the overall verification but not planned for the current increment.
- The effect of this test on models, simulations, or assessments and any subsequent follow-on tests.
- Review of the data collection, data storage, and data processing plan.
- ROE and the plan for post-test restoration of the test environment, test article, or SUT itself.

Review and approval decisions at the authority level required by command guidance are usually set by the residual risk level of the test. Authorities should balance risk against any delay in testing.

Although TRRs may set the boundaries of approval to deviate from or modify a test plan, test teams should resist cost and schedule pressure to modify the test to ensure a "passing" result (i.e., moving the goalposts to guarantee verification). In accordance with DoWM 5000.103, do not modify cyber DT&E plans or make the expectations easier because of anticipation that the system will fail the test. A test that definitively proves a requirement to be unsatisfied is also a valid test.

Cadence Considerations

To support the test timeline, the system developer or the CDT should schedule a TRR after the test plan(s) is (are) approved and the proper resources are in place.

As an example, for a test event occurring in March, the CyWG should request the CDT complete the TRR no later than 30 days prior, in February. In turn, the test team should draft the detailed test plan and submit it for approval in time to support the February TRR. Internal test approval processes may take up to 30 days, so a March test event should have a detailed test plan drafted and ready for review by January.

Additional considerations may be necessary for programs under oversight, as they often require longer lead times and earlier approval dates to coordinate test plans and/or accomplish necessary VV&A activities.

Each T&E-responsible team, whether system developer, government, or some combination, will establish criteria to declare that the TRR is complete and sufficient (sometimes called "exit criteria"). TRR exit criteria should result in the DA approving or denying the test readiness, and the team will either proceed to testing or make corrections and reattempt. Test teams should store their artifacts from test planning through final reporting for future analysis and refinement.

4.6 Artifact Generation

After the *Preparing for Cyber DT&E* activities and tasks are complete, the test team should have an approved test plan clearly defining the SUT for the test event; outlining the anticipated test environment; identifying data collection and analysis tools and processes; discussing potential test risks, limitations, and mitigations; documenting SUT defensive capabilities; and describing how the test team will emulate threat-representative offensive capabilities, if planned for use in the test. The CyWG has scheduled the necessary test infrastructure and the required resources. The test team has the skills, tools, and assets for specialized testing needs. The prepared test has undergone a successful test readiness decision. The CyWG stores all the decisions and artifacts from *Preparing for Cyber DT&E* in the common repository. (Section 2.2.3 has additional information on data management, data sharing, and data repositories.)

Questions for Test Teams to Ask Themselves

- What questions is the team trying to answer during this test? Is the team planning to capture the correct data? Did the team capture the correct information?
- In what way will the data serve to illustrate the fulfillment of requirements (or not)?
- Has the team adequately addressed data classification and plans, including marking data during test observation and when collecting, transmitting, and transferring (in accordance with the SCG) data; marking data resulting from classification by compilation; and marking data to address proprietary information concerns?
- Does the team have tools for ingesting data and to allow the team to develop and defend insights about cyber requirements?
- Does the team have the proper level of storage (in accordance with the SCG), indexing, and retrieval?
- Are proper contracts (such as a DD Form 254) in place to efficiently transfer data from one stakeholder to another? (For example: The team performed penetration testing on the system, but as stated in the DD Form 254, the system developer must first transfer the data to the government sponsor and then to the test team, consequently causing a delay in the sharing of test data.)

If the answer to any of these questions is "No,"
then how will the team address the matter and move forward?

5 Executing Cyber DT&E

Test execution is the culmination of *Preparing* for cyber DT&E for a specific test event. *Executing* turns test plans into T&E results and is the highest technical risk within cyber DT&E.

The objectives of *Executing Cyber DT&E* are as follows:

- Deliver the test stimulus to the SUT in a controlled manner.
- Capture relevant and detailed SUT response data for subsequent evaluation.
- Capture relevant and detailed information about the test itself to aid in reconstruction, repetition, retest, or defense of results.

This section provides insights into key activities and tasks as to how to execute these objectives.

5.1 Inputs

The primary input to *Executing Cyber DT&E* is the approved test plan developed in prior activities and tasks (see Section 4.4) for each event executed. Cyber DT&E should answer questions for program managers. As the test team transitions from *Preparing* to *Executing*, the test team will continue to provide feedback to the program manager's staff about means and objectives. A successful test is not determined by a simple "pass" or "fail" for the SUT; it is a valid test against a worthwhile information flow target with repeatable and well-captured results. These results are the foundation of subsequent analysis and evaluation.

Cadence Considerations

Certain events may require time-sharing of instrumentation, SUTs, and lab facilities. The test team should plan for a schedule margin to account for unforeseen findings or test troubleshooting. Additionally, unplanned complications such as a resource constraint or SUT configuration issue may cause test event cancellation or early termination.

Because test teams across DoW have multiple SUTs in their annual T&E schedule, it is best to plan for a backup event (e.g., a rain date). If a test event is canceled, it is much easier to move to the backup (rain) date than to have a test team attempt to adjust its entire annual T&E schedule to accommodate the situation.

5.2 Activity: Conduct the Test

The following tasks are common steps and considerations for cyber DT&E execution. In cases where the approved test plan and these tasks diverge, test teams should follow the approved test plan.

During *Executing*, test teams may discover data, information, or findings that drive a modification or deviation from the test plan. Within the bounds of safety, law, and regulation, and with the appropriate approvals, the test team may alter the test conduct to account for this

new information. (An example of where discovery learning can alter test activities is when fuzzing results show unanticipated system anomalies, requiring further characterization to rule in/out possible exploitation.)

5.2.1 Task: Perform Setup, Validation, and Checkout

When the test team, article, range, and data collection means are ready for the test event, test teams should get established and oriented to the test environment and begin preparing for the test itself. The test team should review the systems and develop confidence, ensuring that test actions will be controllable and (acceptably) reversible. The team should perform reconnaissance or scans to verify that the MBCRA-hypothesized kill chain and execution path exists and validating the existence of common vulnerabilities and exposures (CVEs).

"Controllable" and "Acceptably Reversible" in Cyber DT&E

- Controllable: The test team knows what system responses are possible and can choose which mission effects to create.
- Acceptably Reversible: If the contract has designated a specific level of post-test performance from the article, the test team can reliably and predictably return the article to the pre-test condition.

5.2.2 Task: Perform Baseline and Risk-Reduction Test and Evaluation

"Test for Score"

Conducting tests to assess and quantify the performance of a system or component against specific requirements and performance parameters.

Once the test team is ready for the test, and the SUT and stimulation and collection systems are appropriately connected and verified to be working, the test team should perform system baselining and risk reduction before test runs for score.

Creating a baseline of the system stimuli and responses, absent any cyber test injects, is an important element to ensure that test results are definitive and that the system pre-test configuration is known. The baseline will enable establishing if a system response (or non-response) is a true response when a cyber test inject is presented. The baseline will also be necessary when reverting the SUT to the pre-test or "clean" configuration. In certain circumstances, baselining may also include hunting for evidence of previous compromises or exploits, such as malicious code, backdoors, or evidence of prior or existing intrusions before cyber testing. The test team should characterize these cases if found, and the appropriate actions should be taken before continuing with the test.

The team should also perform risk-reduction test events to develop confidence in the system response to specific inputs—if the test planning has identified that certain test points need it. Risk reduction is a trial test, perhaps in variations on conditions or configurations of the article,

with additional safety protections in place (e.g., using a signal analyzer to test weapons jettison before dropping real weapons in flight), or other differences. Pre-score tests mitigate three primary risks:

- **Data collection failure**: Risk-reduction events verify that the data collection apparatus is capturing and presenting data according to the test plan.
- **Test escapes**: A test escape occurs when a system exhibits an unexpected response or becomes unrecoverable, or when a stimulus fails to affect its unacceptable targets. Test escapes require further investigation and characterization and might drive deviations from/modifications to the test plan.
- **Safety**: Risk reduction ensures the maintenance of safety bounds during test conduct.

Cyber test teams may also choose to leverage concurrent cyber and non-cyber testing if the configurations and data collection allow. The CyWG should plan for concurrent tests during *Preparing for Cyber DT&E* activities and tasks and refine the plan during execution.

Cyber testing employs a variety of techniques, both adversarial and cooperative. Test teams may need to choose between adversarial and cooperative techniques or incorporate both, depending on the specific requirements and requirement context, and test teams should communicate with their OT counterparts to plan opportunities for integrated testing (see Section 1.6).

Test teams may wish to further explore system responses in replicated versions of the SUT (e.g., on the National Cyber Range Complex (NCRC) or a dedicated cyber test article). Discoveries during *Executing* becomes feedback to the ongoing CyWG *Planning* efforts.

5.2.3 Task: Conduct Test for Score and Capture Test Result Data

When the SUT is in the test configuration and the data collection and stimulus are ready, the test team is ready to conduct the test for score, which will satisfy the validation method and provide evidence for the requirements.

A test with no data collection is a wasted test, so cyber DT&E teams should diligently collect data supporting or refuting the verification. The test plan documents the selection of what to collect and at what points; how to turn the data into meaningful results; and how to store it during execution. Best

Cyber DT&E Data Collection Goals

At the conclusion of the test, the data collection supports two objectives: (1) providing evidence of validating the requirement and (2) providing specifics to the developer to aid remediation. To create a repeatable test, the team or the evaluators combine data captures (packet/ screen/other) and test team notes with the test plan, test cards, and injections. Developers will want the most detailed and specific information possible to remediate findings.

practices include capturing packets directly (e.g., packet captures or parsed Military Standard (MIL-STD)-1553 data words); coordinated time references (for tracing individual causal events); and independent RF captures (if performing RF-cyber testing). Test teams will need to validate that the stimulus planned is truly the stimulus delivered. Direct introspection into runtime decision making or state machine transitions can be beneficial but is often impractical and may violate required test configurations.

Figure 5-1 shows an example data collection form.

Data Collection Form

Area	Details Gathered
Physical access controls	
• "Gates, guards, and guns"	
• Facility access control lists	
• Adherence to procedures	
Personnel and training	
• Operations	
• Maintenance	
• Storage	
• Procedures	
• Manuals	
• Documentation	
ICT supply chain risk management	
• Maintenance	
• Sustainment	
Hardware security	
• Origin	
• In storage	
• In transit	
• Purchase	
Software security	
• Origination/development	
• In storage	
• In transit	
• Updates	
Interfaces to other entities	
• Encryption	
• Zero trust	
Components from outside the system or integrated into the system	
• Commercial off-the-shelf	
• Government off-the-shelf	
Data from outside the system	
• Trusted systems	
• External systems	
Cross-domain solutions	

Figure 5-1. Example Data Collection Form

While collecting test data, the test team should ensure they are capturing relevant context about the SUT, specifically with respect to access, exploitation timelines, and other technical or nontechnical controls. This context sets the conditions for validation of the requirement and guides whether OT can also use the results.

During execution, it may become necessary to change the test plan, as noted briefly in Section 5.2. The TRR should have set the conditions and authorities under which modifications and deviations occur. Test teams should document any unintentional deviations from the test procedures. Teams might discover an unexpected finding that requires more investigation and would proceed within the TRR-ratified limits to capture as much information as possible within the constraints. Test teams may have latitude for "free play" and need to document the chosen paths and why they were chosen. In any of these cases, thorough documentation should also include the reasons for the deviations and the different SUT conditions during test execution.

5.2.4 Task: Determine Test Closeout

Although the test team may execute test events over time, data collection includes finite events gathering specific information to answer a specific question. As part of the test plan, every test team should have a set of criteria to judge when a particular test is complete. This criteria may include whether the test team executed the test under the conditions and stimulus intended, capturing the results well enough to support the conclusions. Test teams will need to decide how long to attempt a particular exploit before logging the results and moving on to a different method or path. The test team should review security classification of the test assets, test data collected, and the testing toolset before test closeout, including the proper data handling procedures and marking.

During *Planning*, test teams should account for any returning test articles requiring verification of a particular configuration. Often, resetting or reloading the software or cabling is a simple task accomplished with the functionals with the authority to ensure that the article is truly ready for reissue.

5.3 Artifact Generation

Test data collection is essential for documenting results, assisting with finding the causes for DRs, and facilitating risk-reduction efforts before testing for score. Data storage is equally critical. Data collection should be in accordance with the test planning documents, either as part of an existing T&E plan or in a dedicated data collection plan. The test team should classify data according to the SCG based on what the data reveals or the compilation of detailed system performance. Data collected may include proprietary elements, and the CyWG and test teams should handle the data appropriately. (Section 2.2.3 has additional information on data

management, data sharing, and data repositories.) Once the test team has captured the data, the data may require processing to be useful for *Evaluating*. The data package should contain the data themselves; the context around the collection, responses to specific stimuli (usually by including logs, scripts, screen captures, and/or test cards); and the test objective that the test team intends the data package to support.

6 Evaluating Cyber Developmental Test Data

During the *Evaluating Cyber Developmental Test Data* activity and tasks, stakeholders analyze execution results and other information in the data repositories to create test reports and to inform decisions such as technical transitions, technical readiness, design reviews, engineering reviews, security decisions, acquisition decisions, knowledge points, releases, and milestones. The primary focus of this section, however, is to provide the best practices for how to perform *Evaluating Cyber Developmental Test Data* in support of *Reporting Cyber DT&E Results*.

Write Once and Use Many Times

The CyWG should consider using evaluations to meet the needs of multiple stakeholders. The CyWG should help test teams and analysts scope the content of evaluations.

6.1 Inputs

Evaluating Cyber Developmental Test Data is dependent on the data, artifacts, and information in the repositories. These items are the object of executing the test event(s), and the test team should note any planned-for information not obtained when drawing conclusions. DoWM 5000.103 contains a more detailed list of inputs.

6.2 Activity: Cyber Developmental Test Evaluation

6.2.1 Task: Organize the Data

Evaluators will review the data needs for their evaluation task; organize the data available; and assemble the data, notes, and supporting data needed to make and defend assertions about the SUT. Evaluators will use analytical tools and methods, guided by the policy and procedures within their chain of command, to build and connect a body of evidence regarding the SUT and the execution results.

STAT During *Evaluating*

The CyWG should include STAT experts as part of the CyWG when evaluating data. These experts use scientific techniques appropriate to the type of data (qualitative, continuous, binary) to analyze the data and rigorously characterize the data's implications for risks to the SUT's cyber resilience and overall cyber capability.

6.2.2 Task: Review Data and Define Evaluation Focus

Evaluators begin by reviewing upcoming decisions, identified needs, and key questions requiring analysis. The CyWG ensures evaluators have access to relevant prior system developer and government test reports within the data repository.

Evaluators should thoroughly review this information, prioritizing the most recent reports, to determine if the collected data adequately addresses the questions and supports the decisions

outlined in the IDSK. (For more information on the IDSK, see Section K.2.7). If sufficient data for analysis is lacking, additional cyber DT&E may be required to inform decision-making.

Evaluators should base their opinions on a well-founded contextual understanding and confirm that the available test results meet the SUT's needs within the defined context. To support this, evaluators should:

- Review related requirements and measures in the traceability matrix (or similar document) associated with the SUT.
- Review planned tests related to the SUT's interfaces, subcomponents, components, or subsystems.
- Review the test plan objectives and related MBCRA scenarios.

6.2.3 Task: Synthesize and Correlate Findings

Evaluators prepare the analytical basis by reviewing historical data within the data repository to provide context for recent findings. Rather than summarizing individual sources, evaluators integrate ideas and findings from multiple sources to develop a comprehensive understanding. They correlate results from cyber DT&E events with existing evidence from MBCRAs, prior test events, and findings from non-cyber systems. Throughout this process, evaluators consider the test environment, the SUT's maturity, the schedule of future events, and the feasibility of implementing fixes and conducting regression testing, as required.

6.2.4 Task: Analyze Performance and Risk

Evaluators perform a comprehensive analysis to assess adherence to security standards, performance against KPPs and technical requirements, and the risks associated with unresolved vulnerabilities, architectural flaws, network issues, or design problems. Measures and metrics used in this analysis should be mission-derived and directly linked to explicit or derived requirements from the SUT. STAT representatives supporting the analysis will assess whether the testing adequately provides the data needed to track progress on technical performance measures (TPMs) and resolve developmental issues. Beyond evaluating the data and measurements, evaluators should also closely monitor the status of deficiencies identified in previous cyber testing.

Common Software Analysis Types

- Defect Analysis
- Root Cause Analysis
- Severity and Priority Assessment
- Decision Making/Feedback Loops
- Validation of Fixes
- Continuous Improvement

Cyber DT&E evaluations should consider all these areas and whether the test data enable completing the report based on the guidance in Table 6-1, adapted from

DoWM 5000.103, when assessing knowledge points, technology readiness, technology transition, milestones, adequacy, schedules, requirements, cyber DT&E events, remediation, mitigations, corrective actions, defender requirements, and cyber posture.

6.2.5 Task: Prepare Conclusions

Upon completion of the tasks described in Sections 6.2.1 through 6.2.4, evaluators prepare conclusions to include in the report in accordance with organizational or DoW Component guidance. *Reporting* cyber DT&E results should provide conclusions, with the supporting evidence (data, analyses, and trends) necessary to support and understand the results. The team should consider alternative explanations, mission impacts, possibilities not tested, and sufficiency of evidence.

6.3 Artifact Generation

Cadence Considerations

Evaluators generate analytical products at a particular time to support a decision point or rolling delivery (such as may align with DevSecOps) to satisfy the necessary role of independent testing in pipeline deliveries.

The evaluators should provide all results of *Evaluating Cyber Developmental Test Data* to the data repository. (Section 2.2.3 has additional information on data management, data sharing and data repositories.) Table provides the data collection focus areas to inform *Reporting Cyber DT&E Results* activities. Each test event's *Evaluating Cyber Developmental Test Data* and *Reporting Cyber DT&E Results* activities and tasks will address a subset (or all) of these data, depending upon the individual events performed during *Executing Cyber DT&E*. The evaluator should always include the sections in Table 6-1 marked with an asterisk.

Table 6-1. Evaluate Data Collection

Section	How to Evaluate
***Test Conduct** (test execution context)	• Analyze the test schedule, the organizations involved, the facilities used, any new or expected limitations or constraints, and deviations from the test plan. • Consider: – Timing: Was the test conducted on the planned timing? Was the test sensitive to timing (e.g., a traffic test performed when there were no users on the system under test (SUT))? – Deviations: Did the test team discover that anomalies impacted the test? Was the venue, range, or test article able to provide enough bandwidth to run the test and the data collection? Did the test team use free play to discover additional risks?

Section	How to Evaluate
	– Organizations: Were there organizational conflicts impacting the conduct of the test? Were there policy impediments (e.g., access to a data repository because it is controlled by another entity)?
***System Configuration** (contextual data about actual system configuration, as tested)	• Analyze the tested versions, configurations, addresses, dataflows, interfaces, protections, etc., and the differences from the expected or planned architectures and configurations. • Note any differences from the test plan and discuss a judgment about whether there was an impact on the verification results.
Cyberspace Attack Scenarios (contextual data describing the threat, including unattributed and defender sources of risk)	• If employed, analyze (record, decide, and publish a judgment about) the adversarial techniques, activities, threat representation level, evidence of success, use of white cards, and impacts of all tested attack scenarios. • Evaluate the mission based cyber risk assessment (MBCRA) scenarios tested.
Information and Communication Technology (ICT) Supply Chain (supply side context)	Analyze, if applicable, any identified areas of weakness in developer processes, tools, and environments; open-source vulnerabilities; checksum variances; effects of environmental triggers; and behaviors whether associated with ICT supply chain white cards or as identified in testing. Analyze, as applicable, observed anomalies in system, subsystem, component, or subcomponent behaviors. Cooperative techniques will examine the consequence of a particular fault in the SUT. Adversarial techniques will seek to cause failure. ICT supply chain faults can also include vulnerabilities in data handling and transit. Judge the sufficiency and efficacy of software and hardware assurance plans, Program Protection Implementation Plans, and obfuscation plans.
***Vulnerability and Exposure Identification – Scans**	Analyze and compare identified vulnerabilities and patching status or plans and severity scores against prior tests. Evaluate trends in vulnerabilities. Compare with known exploitation or current intelligence and with MBCRA findings to correlate the relevance of vulnerabilities to mission- and safety-critical functionality. Ensure that data collection discusses closure (or not) of previous deficiency reports or the status of remediation plans.
Vulnerability and Exposure Exploitation	Analyze the data associated with applicable vulnerability exploitation (e.g., access attained, detections) and exploitation techniques or tools used.
Integrated Cyber Electromagnetic Spectrum Operations (EMSO) Testing	If the test included cyber-enabled EMSO or EMSO-enabled cyber techniques, analyze how the electromagnetic spectrum did or could enable or hinder aggressive cyber activities. Document electromagnetic component architecture in terms of Harvard or von Neumann constructions.
Operational Mission Effects Including Force Protection	Analyze collected, measured, observed, anticipated, or estimated effects of exploitation.
Prevent	Evaluate the evidence of fault-tolerant design features proactively inhibiting risk. Evaluate evidence of software assurance, hardware assurance, and protection features that increase code or design

Section	How to Evaluate
(proactive actions, identify, protect)	quality. Evaluate proactive defense measures such as port hopping, firewall access control lists and process, data diodes, and rejection of scanning queries.
Mitigate (detect, contain, eliminate, system monitoring)	• Correlate the inherent (baseline truth) and inherited (deltas) cyber defenses with anomalies; cyber actions or cyberspace events prevented and the means of prevention (success); the mechanism used to detect or discover the actions (e.g., cyber defender, automated notifications, or monitoring) and anomalies; and cyber actions or cyberspace events not prevented (failures) requiring mitigation, containment, elimination, or recovery of mission- or safety-critical functions. • Analyze the collected evidence, measurement, techniques, and effectiveness of detections, containments, elimination of incidents, and system monitoring capabilities.
Mitigate (system response actions)	Analyze the collected evidence, measurement, techniques, and effectiveness of SUT or proxy operator response capabilities.
Recover or Adapt (system or operator recovery or adaptation and restoration actions)	Analyze the collected evidence, measurement, techniques, extent (full or decremented), and effectiveness of anticipated (or actual) restoration (recovery of affected SUT functions) capabilities.

7 Reporting Cyber DT&E Results

The objective of *Reporting Cyber DT&E Results* activities is to clearly communicate to decision makers and stakeholders the test team's judgment, the evaluation assessment (risks, mitigations, etc.), and the required specific data to substantiate the assertions. *Reporting Cyber DT&E Results* also delivers updates to the relevant SUTs and informs subsequent or in-progress *Iterative Planning and Preparing for Cyber DT&E* for the relevant systems tested. Cyber DT&E reports should serve one or more of the following purposes:

Data Classification

Aggregation of system or mission documentation and test data often raises the classification. Use the SCG for derived marking, safeguarding, storage, and dissemination of reports.

- Verify requirements.
- Characterize the SUT's cyber posture.
- Communicate the SUT's cybersecurity and cyber resilience performance, including publishing risks, DRs or watch items.
- Inform decisions (e.g., programmatic, design, engineering, security, risk, integration, transition, authorization, and operational decisions).
- Communicate the limitations of cyber DT&E; the conduct of prior and future *Executing Cyber DT&E* activities; the scope of cyber DT&E (what needs iterating, mitigating, or remediating or is adequate to move on to OT&E); and any remaining unknowns.
- Satisfy the verification step of an MBSE management approach, satisfy testing steps within a DevSecOps pipeline development approach, or both.

If test teams are writing a report whose primary focus is to simply report on requirements progress, they should review the *Executing Cyber DT&E* in Section 5 because the test plan and report generally mirror each other. For larger or more wide-reaching reports (e.g., leading up to a major milestone or minimum viable product delivery), test teams can expect to perform more synthesis and aggregation of results.

STAT Role During *Reporting*

The CyWG should include STAT experts as part of the CyWG when producing reports. These experts can help provide rigorous connections of the data to the evaluation results for the system's cyber capability and provide information on the limitations, scope, and coverage of the T&E.

Each stakeholder should be able to access all *Reporting* information.

The last step in *Reporting Cyber DT&E Results* is to update organizational data repositories with the new report and disseminate it following organizational procedures, in accordance with DoWM 5000.103.

7.1 Inputs

In executing the test plan, test teams ensure that the outputs of the *Reporting Cyber DT&E Results* fit the needs of the primary stakeholder or activity resourcing or requesting the T&E event(s). DevSecOps developers may require very focused and short input test results, such as the results of a periodic test script and the findings added to the backlog or forward-work entries for DevSecOps teams to handle as chores. In contracts, a major acquisition program may have quarterly reviews of requirements sell-off and DR resolution tracking, for example. DR fix verification may have very narrowly focused *Executing* and *Evaluating* criteria. Reports should consider each section in Table 4 of DoWM 5000.103. Sections not applicable to the specific report should provide a brief non-applicability explanation. Test teams should feel empowered to structure the reports in a way to best achieve organizational objectives.

7.2 Activity: Develop Cyber DT&E Reports

Test teams typically complete the following activities in producing a cyber DT&E report:

1. Gather outputs from *Evaluating Cyber Developmental Test Data* activity tasks and supporting artifacts (current, prior, other relevant systems).
2. Decide the security classification level for the finished report. A fully populated report will likely specify the mission impact of potential vulnerabilities and detailed means of triggering, which the test team has tested and confirmed. Aggregation, "publishing recipes," and confirmation of vulnerability effects often change the classification level.
3. Describe the findings in a relevant, supportable, and concise way. Test teams should ensure that the report includes sufficient details for the developers to reproduce, find, and remediate the issue, if possible.
4. Complete the report, whether in prose or some other delivery format, such as through MBSE-integrated platforms or by updating tickets in a software development tracking

Cadence Considerations

T&E personnel should be able to draft much of the report in parallel with the test plan because these documents will mirror each other, and the plan exists to satisfy the needs of the report.

As the test team collects and refines the results, and the evaluation results begin to formulate, test teams will be able to start populating the remaining sections of the report with assertions, data, and conclusions.

system. Ensure that the report covers required items in DoWM 5000.103 or acknowledges/ justifies deviations. Enter DRs (if any) into the appropriate deficiency data repository of record, whether it is the Joint Deficiency Reporting System or the system developer's backlog management tool (e.g., Jira) (or another repository if required by the local policy).

5. Perform review and publishing processes as appropriate to the SUT and test ecosystem.
6. Develop recommendations for future testing, fixing, and retesting and the status of the fixes.

Cyber DT&E reports should describe the following in terms the program manager and developers can understand:

- System or mission impact of any deficiencies.
- Positive features of the design, capabilities, or mitigations.
- STIG compliance issues as described in DoWM 5000.103. SNCR—system not in compliance with requirements—status should be linked to potential mission impacts, if any, and provided to the team responsible for overseeing the SUT's DoW RMF process, including:
  - Security controls that are not met.
  - Identified vulnerabilities (see Table 7-1) that are:
    - Not accessible.
    - Accessible but not in a timeline that could affect missions (e.g., crypto).
    - Accessible in mission-relevant timelines but not exploitable.
    - Accessible and exploitable but not in mission-relevant timelines.
    - Accessible and exploitable in mission-relevant timelines but will not impact mission-critical functions (e.g., designed heterogeneous fault tolerance).
    - Both accessible and exploitable within mission-relevant timelines.

Example: Naval Air Systems DR Impact Categorization

Part I
- Major safety or mission impact.

Part II
- Moderate mission impact.

Part III
- Minor operator compensation required.



Table 7-1. Vulnerability Class

	NOT Mission-Relevant Timelines	Mission-Relevant Timelines
Mission-Relevant Data NOT Accessible	Information is not accessible; also, exploiting information will not compromise the mission	System access is possible in a mission-relevant time; no mission-relevant information exposed
Mission-Relevant Data Accessible	Data Accessible but Not Exploitable in time (often encrypted)	Data Not Exploitable
	Mission Data Exploitable, but not in a mission-relevant time	Data Exploitable, but mission execution is resilient (e.g., designed heterogeneous fault-tolerant functionality)
		Data Exploitable in a mission-relevant time

Additional considerations when writing reports, independent of the system's specified requirements, include:

- System successes or failures at providing indications to the operator or maintainer of any breach, data exfiltration, intrusion, or unauthorized changes to the data or software configuration.
- Whether system users can or cannot restore the system to its operational condition in a mission-relevant timeline following a breach, intrusion, or unauthorized change to the data or software configuration.

7.3 Artifact Generation

Reporting Cyber DT&E Results, performed by test teams, uses the data repository and *Evaluating* results to inform decision or knowledge points and stakeholder requirements. (Section 2.2.3 has additional information on data management, data sharing, and data repositories.) *Reporting Cyber DT&E Results* activities should consider data from more than one source or test. *Reporting* evaluation results should provide conclusions, with the supporting evidence (data and analyses) necessary to support and understand the results. DR reporting is the responsibility of the CyWG and should be in accordance with the organization's DR process. Table 7-2 recommends the data to include in *Reporting*.

Table 7-2. Cyber DT&E Assessment Considerations for Stakeholder Reporting

Standard Report Items	
Admin	• Name(s) of the test team.

	• Date of the report. • Program or project name or the name of the test. • Distribution and/or classification statements.
Background and Context for the Test	• Authority for conducting the test. • T&E dates. • Associated DT&E plan(s). • Requirements for verification. • Scope (what was in, what was out).
Test Conduct	• System under test (SUT) configuration and details (version numbers, network architecture, configuration settings, etc.). • Details about the data collected and how they relate to *Evaluating*, measures, and metrics. • Test tools and setup: How was the SUT controlled and stimulated (ranges, harnesses, "twins," etc.)? • Test itself: Detailed method of test/detailed test procedures, rules of engagement • Deviations: how the test went differently than planned, whether those differences matter to the T&E. • Results: SUT response in a specific configuration given those inputs (e.g., expected response and observed response).
Evaluation	• Test team evaluation, and how the results justify the evaluation. • Mission impacts of the findings. • Decision, knowledge point, or milestone supported. • Inputs to the deficiency report or watch item process (if appropriate). – Categorize deficiencies in terms of the expectation or feasibility of fixing: for example, fix as soon as possible regardless of cost (high impact and high likelihood); add to the backlog and fix in a future update; impossible to fix—develop tactics, techniques, and procedures to detect and mitigate. • Defense Information Systems Agency or cyber survivability attribute categories and severity levels (if appropriate).

Additionally, the CyWG may need to adjust the TEMP or T&E strategy as the test teams refine individual test plans and execute test events. Report results may affect the overarching cyber DT&E strategy. The CyWG should provide its updates to the TEMP or other T&E strategy, IDSK (see Section K.2.7), and any supporting documentation as part of the iterative nature of cyber DT&E.

7.4 Evidence/Data Management

From *Iterative Planning for Cyber DT&E* through final *Reporting*, the CyWG is responsible for comprehensive data management throughout the system lifecycle. Effective data management relies on distinct processes for data discovery, collection, and storage, enabling enterprise-wide

access to federated data and promoting the collective sharing of data and assurance evidence. The JETEP Website (https://jetep.apps.dso.mil/) serves as a central resource for discovering assurance evidence, data, and sources from across the federation, including test, evaluation, and engineering data. JETEP supports the collection and aggregation of engineering data across the system lifecycle, allowing the CyWG to develop a federated, evidence-based, and holistic assurance approach to support effective risk-based decision-making. This integrated approach connects data, digital information, and assurance evidence to decisions, informing technical risk assessments for systems both before and during fielding to operational activities.

8 Cyber DT&E Process Challenges and Digital Engineering Considerations

This section focuses on managing the challenges that a CyWG may encounter in executing the cyber DT&E process for non-acquisition, pre-acquisition, and acquisition approaches and foreign-acquired systems. These challenges are areas that the CyWG should understand from a cyber risk to mission perspective when prioritizing and scoping cyber DT&E during *Planning*. This section provides considerations in DE including using digital twins, M&S, and cyber analytic tools in support of the cyber DT&E process.

Many factors could influence the cyber DT&E process; non-exhaustive examples include:

- Anticipated or existing software and hardware updates.
- Complexity of the technologies or system(s) (e.g., individual technology, networked system versus non-networked, SoS, platform of systems).
- Data rights and the ability to reverse engineer.
- DoW Component-specific policies, procedures, and guidance.
- Existing versus new system developer contracts.
- Existing versus planned funding.
- ICT supply chain visibility and risks.
- Maturity of the system (e.g., legacy versus new concept).
- Measurable and testable cyber requirements.
- Mission(s).
- Modular open systems approach.
- Pace of development.
- Urgency of need.
- Use of DE.

Remember: This guidebook contains generalized content. Because of the unknown range of factors for each development effort including non-acquisition, pre-acquisition, and acquisition, this section cannot be exhaustive or comprehensive.

8.1 Non-Acquisition and Pre-Acquisition

In accordance with DoWM 5000.103, projects such as non-acquisition and pre-acquisition program technology, S&T, prototyping and experimentation, and any development for eventual insertion into DoW networks, systems, platforms of systems, and SoS should implement versions of the processes discussed in this guidebook and tailored to their content and timelines consistent with ensuring cyber resilience. The scope may be potentially smaller with less complexity than the scope of a POR, depending upon the effort. Cyber requirements are usually not defined at all for research efforts, but the research efforts should still strive to ensure cyber resilience is an early consideration, to derive requirements based on the DoDI 8500.01, and implement the cyber DT&E process to verify those requirements. The CyWG's *Planning* priorities include:

- Performing an early MBCRA. The MBCRA delivers the greatest benefit to the CyWG's scoping efforts and understanding of overall risk because of anticipated limited cyber testing opportunities.
- Analyzing the maturity of the effort and the trajectory for insertion into DoW networks, systems, platforms of systems, and SoS to inform scoping the cyber DT&E strategy and developing the IDSK. For more information on the IDSK, see Section K.2.7.
- Considering following the UCA pathway which may have similar development timelines. See Paragraph 5.2 (Table 5 and Figure 4) of DoWM 5000.103 and Section 8.5.1 in this guidebook for UCA pathway specifics.
- Working with the engineering team to define cyber performance requirements. The contract should require the system developer to verify meeting the requirements.
- Performing cyber DT&E at the cadence necessary to verify the cyber resilience performance of the technology or prototype.

As the technology develops, the CyWG should pay attention to:

- Understanding and verifying cyber performance and the mission-relevant terrain in contested cyberspace after insertion into a DoW network, system, platform of systems, or SoS.
- Evaluating new cyber risks to or coming from the proposed insertion.
- Understanding areas of risks in the ICT supply chain.
- Assessing resilience against threat-based TTPs.
- Complying with the DoW Cybersecurity Program.

Figure 8-1 is the generic depiction that Section 5 of DoWM 5000.103 uses to represent the agile and iterative nature of the campaign of learning to support the decisions for AAF pathways. Figure 8-1 is applicable to non-AAF efforts and depicts the high-level cyber DT&E activities, shown in Figure 2-1 and discussed in Sections 3 through 7 of this guidebook, as parallel ongoing efforts throughout the life cycle of a system.

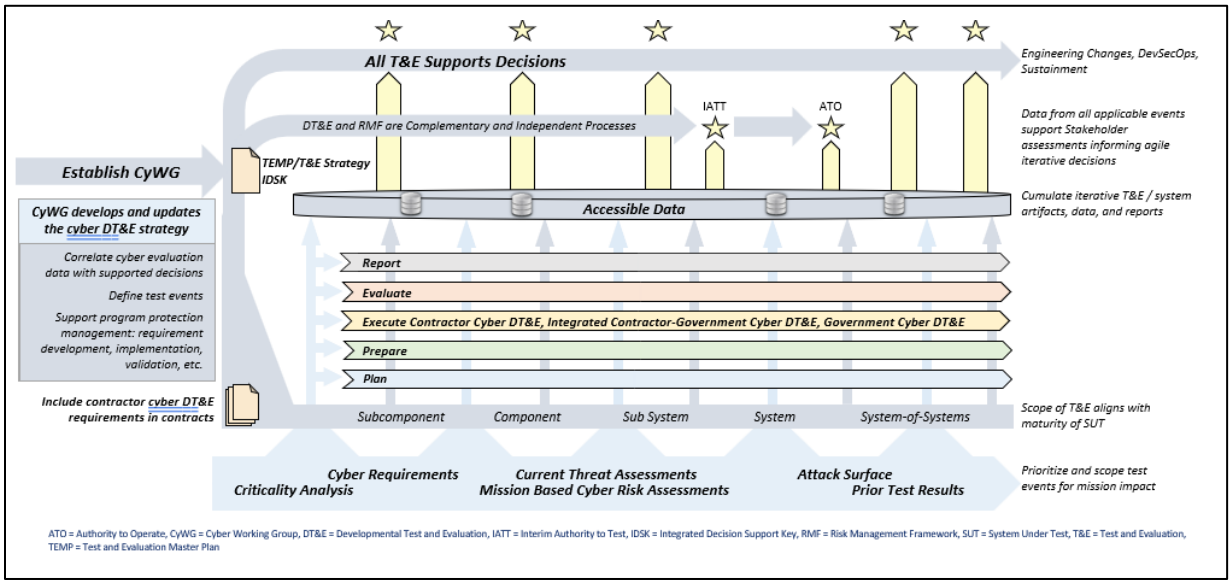


Figure 8-1. Cyber DT&E Activities – A Campaign of Learning to Support Decisions

8.2 Adaptive Acquisition Framework Pathway Considerations

Section 5 of DoWM 5000.103 illustrates the notional timelines across system developer and government cyber DT&E program activities for each of the six pathways.

AAF and DoW RMF

For more information on AAF integration activities, see "Cybersecurity in the Adaptive Acquisition Framework" guidance on the DoW CIO Library Website (https://dodcio.defense.gov/Library/).

8.3 Considerations for Systems, Subsystems, Components, and Subcomponents of Uncertain Pedigree

The acquisition of foreign systems, commercial off-the-shelf (COTS) systems, or other "black box" systems, subsystems, components, and subcomponents of uncertain cyber resilience pedigree can often lead to increased, unknown, and unmitigated risk, regardless of acquisition pathway, acquisition category, contracting model, or program type. These systems or parts of systems either are not undergoing any development or have development efforts that are inaccessible to the CyWG, thus limiting the scope of cyber DT&E. The CyWG should at a minimum partner closely with the program protection team to:

- Seek segmented bills of materials (BOMs) (i.e., SBOM, HBOM) and documented cyber supply chain risk management (C-SCRM) procedures and invest in commercial tools to build BOMs and illuminate the ICT supply chain.
- Conduct an architecture vulnerability analysis and MBCRAs to identify cyber resilience requirements gaps as part of an Analysis of Alternatives or other preliminary capability market research and studies.
- Ensure that cyber DT&E events include threat hunting, penetration testing, and red team exercises.
- Confirm the implementation of cybersecurity tenets (e.g., confidentiality, integrity, availability, nonrepudiation) and compliance with cyber policy and guidance.

8.4 Strategies for Tackling Cyber DT&E Process Challenges

This section describes common cyber DT&E process challenges and provides suggested strategies for addressing each challenge. Reminder: This guidebook contains generalized content. This list is not exhaustive.

Budget

Challenge: The CyWG requires a cyber DT&E budget to support having the necessary technical expertise, cyber test assets, tools, and infrastructure.

Strategies: The CyWG should:

- Request the LDTO establish the cyber DT&E budget as part of the overall DT&E budget.
- Collaborate with financial planners to establish a dedicated cyber DT&E budget line.
- Develop a comprehensive cost estimate for cyber DT&E activities to inform budget planning and resource allocation aligned with system development milestones and critical path activities.
- Prioritize cyber DT&E activities and focuses on the most critical systems and capabilities to maximize the use of limited funds.
- Explore alternative funding sources, such as cyber-specific funding initiatives or partnerships with other organizations, or leveraging external resources, such as contractor support or government agencies.
- Identify systems with similar or identical components or subsystems and request the cyber T&E results.

Continuous Integration and Continuous Delivery

Challenge: The use of automated continuous integration and continuous delivery pipelines is a best practice, but failing to plan and support manual cyber testing during the continuous integration and development process can result in poorly verified cyber requirements. See the DoD Software DT&E in DevSecOps Guidebook (https://www.cto.mil/dtea/software/) for more information.

Strategies: The CyWG should:

- Focus on identifying and prioritizing the cyber requirements for automated testing versus manual testing.
- Define and refine a growing catalog of mission-based cyber test scripts to enable automated dynamic application security testing, use extensive fuzzing, and verify the effectiveness of security fixes.
- Plan to conduct manual cyber DT&E primarily during the test/release, deliver, and deploy phases for major changes in system functionality; plan and conduct manual government cyber DT&E.
- Plan and conduct cyber DT&E of the pipeline manual cyber DT&E events and conduct cyber DT&E of embedded software as integration begins as part of the developmental system's DT&E.
- Ensure that the software factory incorporates continuous monitoring, threat modeling as code, infrastructure as code, and security as code with application program interface (API) testing, static application security testing, dynamic application security testing, and interactive application security testing.
- Review and select security test methods and tools while considering software language, software standards, access to source code, and common weaknesses based on system characteristics.
- Review all automated security T&E results and software assurance assessments to inform manual cyber DT&E.

Contractual Language

Challenge: The contract lacks explicit language requiring the system developer to conduct cyber DT&E. See Appendix I:.

Strategy: Absent the ability to update the contract, the CyWG will need to plan resources to conduct more-extensive government cyber DT&E on subcomponents through the full system.

Cyber Threats

Challenge: Securing timely, reliable, and actionable threat data to inform cyber DT&E is often complicated by issues such as threat evolution, classification, and limited visibility. Cyber threat intelligence (CTI) is necessary to inform the development of realistic and effective test scenarios and threat models and to evaluate vulnerability severity. Additionally, adversaries may have extensive knowledge of the technology (e.g., a non-developmental or commercially available technology) and plenty of time to establish TTPs to exploit known CVEs and common weakness enumerations (CWEs) or to create zero-day exploits. Systems operating in traditional networks are susceptible to the same cyberspace threats reported publicly, including phishing, malware and ransomware attacks, denial-of-service attacks, and others. See Appendix D:.

Strategies: The CyWG should:

- As early as possible, work with DIA or Service/Component intelligence organizations to request threat intelligence and counter-intelligence information related to the identified technologies and organizations involved to understand and characterize adversary capabilities, support MBCRAs, and identify any classified vulnerabilities and weaknesses.
- Establish a cadence for requesting updates to threat intelligence before each cyber test event.
- Leverage open-source intelligence and publicly available information on cyber threats and vulnerabilities to supplement classified intelligence.
- Track known open-source software (OSS) vulnerabilities using the National Vulnerability Database (NVD) and the Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Exploitability eXchange (VEX).
- Seek visibility into all software, libraries, and firmware (software and firmware BOMs).
- Use automated threat intelligence feeds and tools.
- Develop and maintain a threat library or repository.
- Collaborate with other organizations, such as industry partners and academia.

Documentation or Data Rights

Challenge: System development approaches have varying documentation requirements. Development timelines may limit the availability and opportunities for sharing system documentation with the CyWG. Data rights limitations can also impede information exchange. COTS and non-developmental system components may have no useful artifacts. A

lack of needed information common in artifacts such as a requirements document, SEP, requirements verification and traceability matrix, and others may make it difficult for the CyWG to begin and sustain continuous *Planning*. See Appendix C:.

Strategies: The CyWG should:

- Establish the CyWG early to pursue data rights agreements and identify, request, and develop the necessary documentation.
- Develop a data exchange agreement between the system developer and the CyWG.
- Identify and prioritize necessary system documentation and test data for cyber DT&E planning and execution.
- Develop a checklist to guide the collection of required information if the program manager's organization will not develop the documentation.
- Collaborate with stakeholders to create surrogate documentation.
- Leverage existing documentation, such as project plans and research reports or similar systems' documentation.
- Plan several early MBCRAs to gather or generate information and identify gaps and to develop a shared understanding of the system's anticipated capabilities and cyber requirements.

Historic Testing Visibility

Challenge: Visibility into previous test events is beneficial but depends on system maturity, contractual language, and other factors. The CyWG may not have adequate opportunities for visibility into past cyber DT&E on technology, components, development/test environment, processes, tools, and ICT supply chain.

Strategies: The CyWG should:

- Identify and prioritize previous test events and system documentation relevant to cyber DT&E planning and execution.
- Develop a schedule for reviewing completed cyber test results as available.
- Pursue contractual provisions providing cyber test data.
- Pursue government interagency agreements to review cyber test results on identical or similar technology or components.

ICT Supply Chain

Challenge: The ICT supply chain, including development, test, and manufacturing environments, poses continuous, often unknown risks to system developers, suppliers, and maintainers from unknown and undetectable vulnerabilities introduced into systems, networks, and components throughout the life cycle.

Strategies: See Appendix F:.

Integration and Interoperability

Challenge: The integration of new or mature technologies, components, or systems into existing systems and platforms can introduce inherited risks and expand the attack surface. This integration can lead to unforeseen vulnerabilities, interoperability issues, and unanticipated failure modes, making it difficult for the CyWG to verify the security and resilience of the resulting system. See Appendix E:.

Strategies: The CyWG should:

- Ensure continuous *Planning* activities including iterative MBCRAs to identify inherited and new integration risks.
- Examine any inherited security capabilities that may reduce risks.
- Identify and prioritize inherited risks based on system functionality and criticality when characterizing the attack surface.
- Develop and execute comprehensive test plans (system developer, government, integrated, or concurrent (see Sections 1.6 and 1.7)) to evaluate the inherited and integration risks or verify the mitigated risk across the integration and interoperability interfaces.
- Request any prior system developer test and mitigation results for new or mature technologies, components, or systems and interfacing systems in RFPs, contracts, or other agreements.

Personnel

Challenge: The CyWG is inadequately staffed, has insufficient expertise, or lacks the required specialized skills. Cyber DT&E personnel need to have the specialized test skills and knowledge aligned to the technologies used in the system under development. See Appendix A:.

Strategies: The CyWG or lead cyber DT&E organization should, as appropriate:

- Ensure that cyber DT&E team leaders, both contractor and government, are at the Master level.. See Appendix A:.
- Identify and recruit personnel with the required skills and expertise (e.g., aircraft component versus cloud versus enterprise).
- Develop and implement training programs to enhance the skills and knowledge of existing personnel in areas such as cyber threat analysis, penetration testing, and vulnerability assessment.
- Collaborate with other organizations, such as industry partners and academia, to access specialized expertise and skills on a temporary or contract basis.
- Supplement the CyWG or test teams with external resources, such as contractors and consultants.
- Develop and maintain a skills inventory and gap analysis to identify needed training or personnel.
- Establish partnerships to share best practices, expertise, and resources in cyber DT&E. For example, participate in the DoW Cyber Developmental Test Cross-Service Working Group (CyberDT XSWG) ; for more information, contact OSDRE-DTEA-Cyber@groups.mail.mil.

Requirements

Challenge: The lack of measurable or testable cyber requirements creates cascading risks throughout development and engineering and into sustainment of the system. The system needs measurable cybersecurity and cyber resilience requirements that are traceable to the mission and capability and are verifiable during development. NIST SP 800-37 states that RMF controls are not requirements. See Appendix B:.

Strategies: The CyWG should:

- Review and apply the considerations in Appendix B:. Partner with the SSE team to derive missing requirements that are specific, measurable, achievable, relevant, and time-bound (SMART).
- Identify and prioritize cybersecurity and cyber resilience requirements based on system behaviors, functionality, and criticality.

Schedule

Challenge: System development schedules and test timelines vary, which may lead to compressed cyber DT&E timelines for planning and execution. Some systems will be in continuous development and require regular cyber DT&E.

Strategies: The CyWG should:

- Prioritize cyber DT&E planning and execution based on system development milestones and critical path activities.
- Perform an early MBCRA.
- Conduct incremental cyber DT&E to inform subsequent development phases integrating government and system developer tests and concurrent testing focused on verifying system performance and the prioritized areas of risk.
- Focus on high-risk areas and critical system components.
- Leverage automated testing tools and techniques to streamline testing.
- Maximize integrated system developer and government cyber DT&E (see Section 1.6).
- Maximize opportunities for concurrent cyber DT&E with non-cyber functional T&E.
- Plan integrated cyber T&E (see Section 1.6) as acceptance testing and closely track all deficiencies and fixes.

Sustainment and Legacy Systems

Challenge: Some legacy systems and platforms continue to need cyber DT&E because of changes, as documented in Paragraph 3.2.a.(13) of DoWM 5000.103, while in sustainment, resulting in possible challenges for the CyWG to obtain funding and add these events to product support strategies or sustainment plans.

Strategies: The CyWG should;

- Integrate cyber DT&E into updates to sustainment plans and product support strategies, including regular cyber DT&E for system updates and changes.
- Develop a sustainment plan that includes regular cyber DT&E activities, such as vulnerability scanning and penetration testing.
- Identify and prioritize high-risk areas and critical system components for sustainment-focused cyber DT&E.

- Consider leveraging automated testing tools and techniques to streamline sustainment testing.
- Request any prior system developer test and mitigation results in RFPs and in contracts.
- Identify modular open-systems approaches to assess the ease and effectiveness of hardware and software updates or refreshes during the system's life cycle.

Test Infrastructure, Facilities, Tools, and Environments

Challenge: Inadequate required test resources or a lack of access to the resources may make it difficult to create realistic and effective test scenarios, simulate real-world cyber threats, and thoroughly evaluate the cybersecurity and resilience of systems and capabilities. See Appendix J:.

Strategies: The CyWG should:

- Identify and leverage existing test facilities, such as government-owned labs or commercial cyber test ranges.
- Develop partnerships with other organizations, such as academia or industry, with the required tools or facilities.
- Invest in the development of digital representations and virtual test environments to simulate real-world scenarios and reduce the reliance on physical test facilities.
- Identify common test tools, facilities, and equipment supporting similar efforts.
- Explore the use of cloud-based or containerized test environments.
- Plan early to use cyber test ranges.
- Negotiate the use of contractor facilities, tools, or equipment.

Use of Commercial Off-the-Shelf and Open-Source Software

Challenge: The use of COTS and OSS components in system development can present challenges such as a lack of ICT supply chain transparency, the presence of existing vulnerabilities, an inability to reverse engineer, and insufficient developer support, potentially compromising security and integrity and increasing the risk of attack. Additionally, OSS may introduce additional risks due to the lack of centralized control, unclear ownership, and potential for malicious code injection. The system developer may not have adequate visibility into the COTS and OSS components, making it difficult to assess and mitigate risks.

Strategies: The CyWG should:

- Develop a COTS and OSS cyber DT&E strategy for prioritized COTS and OSS components.
- Request documented procedures for identifying and mitigating the risks associated with OSS, such as:
  - Identifying and tracking OSS components used in the system.
  - Monitoring OSS vulnerabilities and updates.
  - Implementing measures to prevent malicious code injection.
  - Conducting regular security reviews and audits of OSS components.
  - Developing plans for responding to OSS vulnerabilities and exploits.
  - Using OSS alternatives or proprietary solutions when necessary.

8.5 Model-Based Systems Engineering and Digital Engineering

Digital Engineering

DoDI 5000.97 describes digital engineering (DE) as a means of using and integrating digital models (e.g., MBSE) and the underlying data to support the development, T&E, and sustainment of a system. It involves implementing the following elements:

- DE ecosystem
- Digital models
- Digital twins
- Digital threads
- Digital artifacts

MBSE is the formalized application of modeling to support the system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout the development and later system life cycle phases. The CyWG should collaborate with the system developer and SE team to enable cyber DT&E. The CyWG may be able to use the MBSE environment and government cyber analytic tools to conduct regular analysis of technical designs. The collaboration may improve the consistency of knowledge, identification of early cyber deficiencies, mitigation or remediation of risks, and early cyber DT&E via M&S using shared digital models.

The CyWG should understand any DE efforts. A consideration for enabling early and recurring cyber DT&E may be to use digital twins and M&S, even if the program manager's organization is not implementing MBSE. In accordance with DoDI 5000.61, "DoD Modeling and Simulation Verification, Validation, and Accreditation," acquisition programs will conduct VV&A for the intended use of all digital models, simulations, and associated data.

8.5.1 Digital Twins in Cyber DT&E

Digital twins can be a powerful tool for testing and analyzing complex systems and can support a wide range of cyber DT&E activities. Digital twins can support the comprehensive and relevant cyber vulnerability research of cyber physical systems and enable deep introspection and event retrospection of system components. A digital twin, if sufficiently planned for cyber T&E usage is endlessly reusable.

Considerations

- Digital twins integrate as components of a system in a system integration lab (SIL), a hardware-in-the-loop (HWIL) facility, a cyber range, or another test asset.
- Digital twins can sustain cyber DT&E throughout the life cycle, including dedicated fuzzing over large input parameters; the emulation of destructive adversary capabilities; the assessment of cyber risks to and from interoperable, integrated, or connected systems, SoS, families of systems, and platforms of systems; and the ability to evaluate new vulnerabilities and cyber test changes or updates.
- Digital twins should be a multi-resolution model with exact bitwise accurate instruction processing and time resolution where required to support cyber vulnerability research and exploitation, mitigation response testing, and remediation effectiveness verification and studies.
- Investing in digital twins and sustaining their configuration for cyber DT&E may be more cost-effective than buying test assets that may not enable any destructive or repeatable cyber testing.
- The digital twin should have sufficient fidelity and accuracy before using it for cyber test.
- The CyWG should maintain configuration control of digital models and digital twins supporting cyber DT&E in accordance with DoDI 5000.97, “Digital Engineering.”
- The program management organization should perform digital twin VV&A in accordance with DoDI 5000.61 to ensure the accurate reflection of real-world behavior.
- The CyWG should plan to use digital twins in conjunction with physical testing, rather than replacing it entirely.
- The CyWG should seek to understand the assumptions and limitations of the digital twin and scrutinize the results in the context of these limitations.

Potential Limitations

- Lack of physical realism. Digital twins are simulations and may not perfectly capture the behavior of physical systems. Digital twins may not account for all the nuances and complexities of real-world physics, materials, and interactions.
- Inability to fully replicate human behavior. Digital twins can simulate human interactions but may not fully capture the complexity and variability of human behavior, such as decision making, emotions, and social interactions.
- Limited scope. Digital twins designed to simulate a specific system or process may not be able to capture the broader context or interactions with other systems.
- Dependence on data quality. Digital twins are only as good as the data they are based on. If the data are incomplete, inaccurate, or outdated, the digital twin may not accurately reflect the behavior of the physical system.
- Lack of transparency. Digital twins can be complex and difficult to understand, making it challenging to identify the underlying assumptions and limitations of the simulation.

Risks

- Overreliance on digital twins can lead to a lack of physical testing and validation, which can increase the risk of errors or lead to unexpected behavior in the physical system.
- Without VV&A of digital twins against physical systems to ensure the accurate reflection of real-world behavior, the digital twin may not be reliable.
- Digital twins themselves can be vulnerable to cyberspace attacks, which can compromise the integrity of the simulation and potentially impact the physical system.
- Digital twins may require access to sensitive data, which can raise concerns about data privacy and protection.
- Digital twins in support of cyber T&E are still a relatively new technology, and there is a lack of standardization in their development, deployment, and use. This nascency can make it challenging to compare different digital twins and to ensure their effective use.
- Digital twins are based on assumptions about the behavior of physical systems, and these assumptions may not always be accurate. If the assumptions are incorrect, the digital twin may not accurately reflect the behavior of the physical system.
- Digital twins may not be able to accurately simulate rare events or unexpected behavior, which can limit their ability to predict and prepare for potential risks.

8.5.2 Modeling and Simulation in Cyber DT&E

Using MBSE models, not digital twins, and simulations to conduct cyber DT&E may save resources by allowing for earlier and more frequent testing, reducing the need for physical prototypes and enabling more efficient and effective early analysis of complex systems.

8.5.2.1 Model-Based Systems Engineering and Cyber DT&E

MBSE is an SE approach that uses graphical models to design, analyze, and validate complex systems. By using MBSE models, the CyWG can plan to conduct cyber DT&E earlier in the development process, reducing the risk of costly redesigns and rework. The CyWG can use MBSE models to:

- Analyze system architecture and identify potential vulnerabilities and weaknesses.
- Simulate system behavior and measure the impact of different attacks and scenarios.
- Evaluate system performance and identify potential bottlenecks and areas for improvement.
- Conduct trade studies and evaluate the effectiveness of different cybersecurity implementations.

8.5.2.2 Simulations and Cyber DT&E

Simulations can support cyber DT&E by allowing for the evaluation of complex systems and scenarios in a virtual environment. The CyWG can use simulations to:

- Test and evaluate the effectiveness of different cybersecurity implementations.
- Analyze system behavior under attack and identify potential vulnerabilities and weaknesses.
- Evaluate cyber resilience and identify areas for improvement.
- Conduct what-if analysis and evaluate the impact of different attacks and scenarios.

WU Course CYB 0060, "Benefits of M&S in Cyber T&E"

This course is part of the forthcoming optional Cyber T&E Foundational Credential pathway. For more information, visit https://www.dau.edu/credentials.

8.5.2.3 Benefits of Using MBSE Models and Simulations

Using MBSE models and simulations to conduct cyber DT&E can provide several benefits, including:

- Cost savings. MBSE models and simulations can reduce the need for physical prototypes and minimize the cost of T&E.
- Increased efficiency. MBSE models and simulations can enable more efficient and effective analysis of complex systems, reducing the time and effort required for T&E.
- Improved accuracy. MBSE models and simulations can provide more accurate and reliable results than physical testing, reducing the risk of errors and rework.
- Enhanced collaboration. MBSE models and simulations can facilitate collaboration and communication among stakeholders, ensuring alignment toward common goals.

8.5.2.4 Best Practices for Using Models and Simulations

To get the most out of MBSE models and simulations, it is essential to follow best practices, including the following:

- Develop a comprehensive model that includes all relevant system components and interfaces.
- Use validated and verified models to ensure that the results are accurate and reliable.
- Conduct regular updates and maintenance to ensure that the models and simulations remain current and relevant.
- Provide training and support to ensure that stakeholders understand how to use the models and simulations effectively.

Cyber Data Exchange Model

The Simulation Interoperability Standards Organization (SISO) established the Cyber Data Exchange Model as an open, international standard for the exchange of data about cyber events and objects between kinetic simulations, cyber simulations, and cyber ranges.

(See the SISO Standards Products Website at https://www.sisostandards.org/page/StandardsProducts.)

8.5.3 Cyber Analytic Tools Support CyWG Activities

DE can enhance CyWG planning using automated cyber analytics. Human-centered cyber analysis alone cannot address the scope of the complexity and complicated aspects of DoW systems. Several automated cyber analytics, built and sustained by DoW-sponsored Federally Funded Research and Development Centers (FFRDCs), University-Affiliated Research Centers (UARCs), and commercial companies, ingest digital models to perform analysis of a system. These automated cyber analytics can inform cyber DT&E scope. Employing a data analysis plan and data schema enabling modeling of the cyber requirements, prioritized behaviors, and both defensive and adversarial activities at the onset of model or system creation significantly

enhances the modeling process. Knowing the specific data requirements from the start helps modelers understand the purpose behind each element in the model, rather than merely adhering to general principles. Retrofitting a schema into well-established models presents challenges and may meet resistance from projects with extensive existing frameworks because of the complexity and potential disruptions involved.

Cyber Analytic Tools Rolodex

To search for, learn about, and share cyber T&E supporting tools, facilities, and service providers, go to https://jetep.apps.dso.mil/cyber_te.

For more information, contact OSDRE-DTEA-Cyber@groups.mail.mil.

The CyWG should use automated testing and analytics to the greatest extent possible for the efficient gains to augment human judgment. Humans should adjudicate the findings and continuously evaluate whether a false negative rate is creeping into the system. Not all automated analytics can provide meaningful analysis to inform the cyber DT&E scope before a system design exists. Therefore, the CyWG should not adopt automated cyber analytics without understanding the potential limitations and should consider a suite of analytics to ensure breadth in the analytic approaches.

8.5.4 Leveraging Ontologies for Enhanced Cyber DT&E in MBSE and DE

Modern DoW systems are becoming increasingly complex, and this complexity is managed through MBSE and DE approaches. These approaches rely on interconnected models representing system elements, behaviors, and relationships. Models alone, however, are not sufficient. DoW also needs a shared, formal understanding of the meaning behind the data within those models. Ontologies enable this understanding.

An ontology defines a common vocabulary for a domain, for example, cybersecurity, testing, and evaluation. It explicitly specifies concepts, properties, and the relationships between them as a structured knowledge representation. Unlike a simple data dictionary, an ontology incorporates logical rules and constraints, enabling reasoning and automated inference.

For example: A data dictionary might list “vulnerability” as a text string. An ontology provides a common, traceable definition and may include *relationships* to other defined ontology items such as *has a* ““Common Vulnerability Scoring System (CVSS) score,” *affects a* “system component,” and *mitigated by a* “patch.” This richer definition allows systems to understand and act upon vulnerability information more intelligently.

8.5.4.1 Why Ontologies Matter for Cyber DT&E

Ontologies can significantly improve the effectiveness and efficiency of cyber DT&E within MBSE/DE environments. They can deliver benefits across several key areas:

- Enhanced data quality and consistency. Ontologies enforce data consistency through defined relationships and constraints. This consistency minimizes ambiguity and errors, leading to more reliable analysis and test results. The system validates data against the ontology, ensuring that it conforms to established definitions.
- Automated reasoning and analysis. Ontologies enable automated reasoning. DE, MBSE, and cyber analytic tools can infer new knowledge from existing data. For example, if a vulnerability affects a critical system component, the ontology allows the automatic identification of potential mission impacts. Automation accelerates risk assessment and prioritization.
- More effective threat modeling. Ontologies support the creation of robust threat models. By representing threats, vulnerabilities, and attack patterns within the ontology, the tools can perform more comprehensive analysis and identification of potential weaknesses.
- Streamlined reporting and communication. A shared ontology provides a common language for reporting the analysis and T&E results and communicating the findings to stakeholders, improving clarity and reducing misunderstanding.
- Knowledge capture and reuse. Ontologies capture valuable cyber knowledge to maximize reusability across different projects and systems and minimize reinventing the wheel by leveraging prior experience and knowledge.

8.5.4.2 Ontologies That Support Cyber DT&E

One of the ontologies that exists to support cyber DT&E is MITRE's publicly available Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND) (https://d3fend.mitre.org/).

The Ontology for Attacks in Cyber Risk Assessments (OACRA) Viewer, prototyped by the Office of the Under Secretary of War for Research and Engineering, Technology Readiness Level 5, is an ontology to support MBCRA data reuse. One problem is that DoW Components do not have a consolidated and reusable repository of known attack methods via attack vectors from across services, platforms, or programs that enables information sharing and machine reasoning in the cyber domain. Without a machine-readable knowledge model of cyber targets and cyberspace attacks via specified attack vectors, DoW Components cannot comprehensively conduct analysis of and testing for cyberspace risks for DoW systems. DoW Components primarily use manual efforts relying on limited human knowledge and expertise. The effectiveness of the analysis and testing is dependent on SME availability.

The OACRA Viewer approach for addressing the problem is to field the critical technology to mitigate the complexities of an exponentially evolving cyber ecosystem through advances in

knowledge curation and data enrichment that expands and informs actionable information. Figure 8-2 depicts the original system view for the OACRA Viewer.

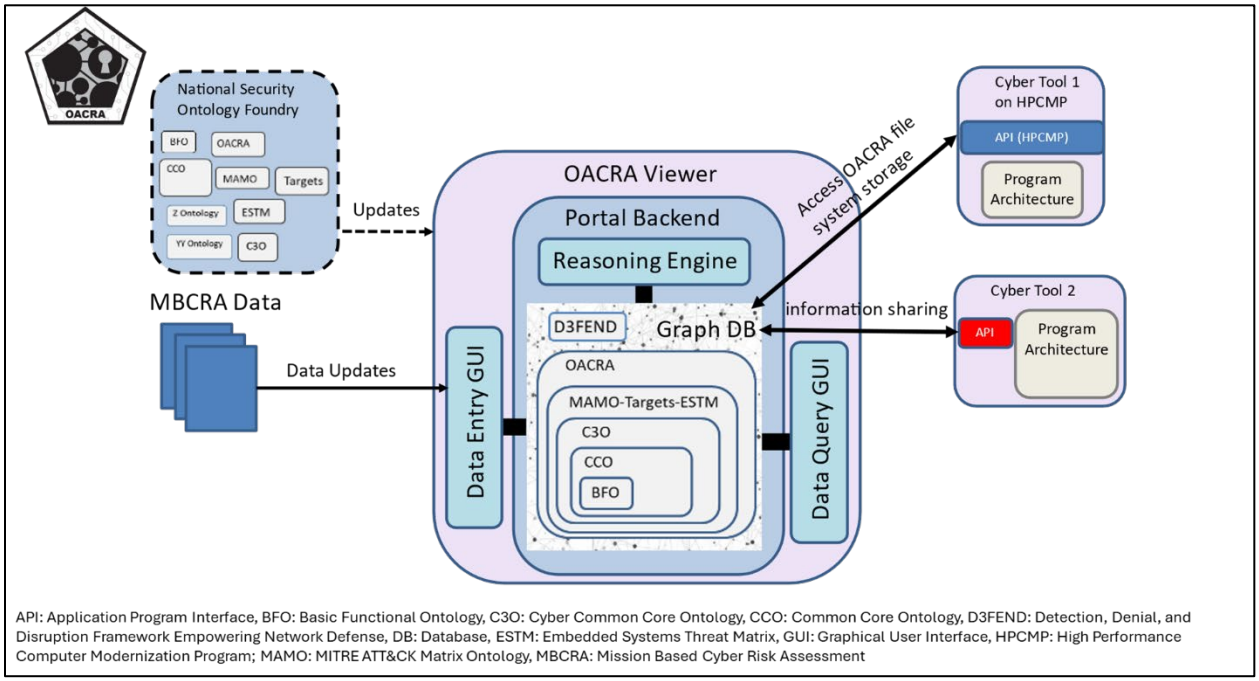


Figure 8-2. The OACRA Viewer Systems View

The OACRA Viewer seeks to employ an ontology of attacks together with the ability (through a user interface or APIs) to curate, search, and add additional attack procedure instances to the ontology. OACRA advances the modeling of cyberspace attacks enabling DE to enhance cyber risk assessments. It promotes collaboration and information sharing and reduces the dependency on human availability, knowledge, and expertise.

The underlying ontology is under revision. The OACRA Viewer currently operates on the DoW High Performance Computing restricted Army Research Laboratory's portal using a backend portal to update, manage, and distribute the ontology and information, providing a common platform for user access and data sharing. For access to OACRA, contact OSDRE-DTEA-Cyber@groups.mail.mil.

Other related ontology resources include:

- World Wide Web Consortium Data Activity (https://www.w3.org/2013/data/).
- Organization for the Advancement of Structured Information Standards: Structured Threat Information Expression and Trusted Automated Exchange of Intelligence Information (https://www.oasis-open.org/2021/06/23/stix-v2-1-and-taxii-v2-1-oasis-standards-are-published/).

Appendix A: Considerations for Staffing Cyber DT&E Activities

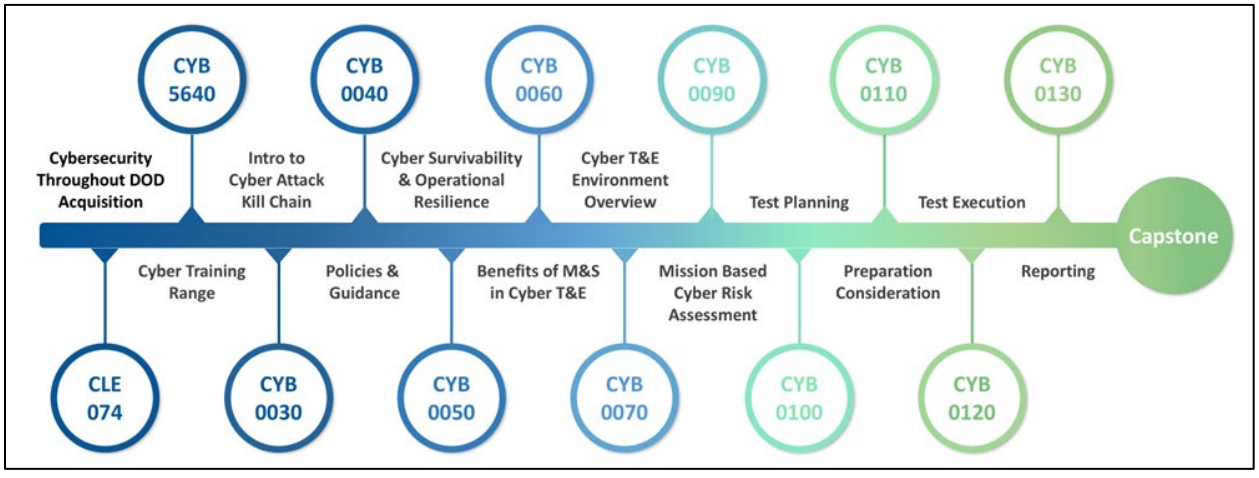
A.1 Purpose

This appendix provides guidance for identifying and staffing cyber DT&E personnel and outlines the qualifications for various roles involved in successful cyber DT&E execution. It also covers key aspects such as the CyWG, which is responsible for overseeing cyber DT&E efforts; strategies for maintaining workforce proficiency; and where to find a current list of T&E organizations.

A.2 Roles Supporting Cyber DT&E

No two systems or test events will require the exact same cyber DT&E; therefore, the program manager should carefully consider the skills and knowledge of the personnel supporting the system for cyber DT&E. Cyber DT&E personnel should have experience in the protocols and architecture associated with the system. For example, if the system or subsystem is an Internet-based platform using COTS-based software and hardware, then the test team should have previous experience with both web-based platform testing and the specific COTS product. On the other hand, if the system or subsystem is an industrial control system with non-IP-based communication, then the desired cyber DT&E personnel should have prior experience in industrial control systems.

Figure A-1 depicts the entire set of courses to satisfy the WU Cyber T&E Foundational Credential.

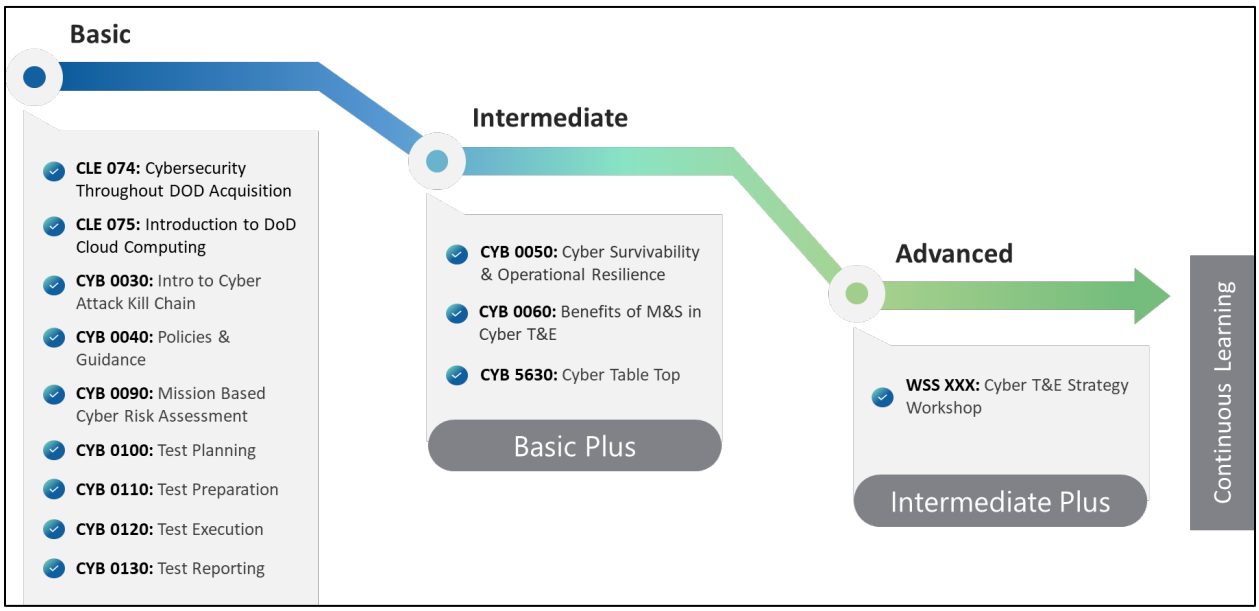


Source: Warfighting Acquisition University

Figure A-1. WU Cyber T&E Foundational Credential Pathway, Under Development

The following subsections describe the roles typically needed to plan and conduct cyber DT&E. The system developer contract should include provisions for the desired knowledge, skills, and

abilities or DoW Cyber Workforce Framework (DCWF) roles that the developer will employ for system developer planned and performed cyber DT&E. All CyWG representatives should strive to earn the WU Cyber T&E Foundational Credential, which is under development and depicted in Figure A-1. At the time of this guidebook's publication, not all courses are available. At a minimum, the CyWG participants should complete the proposed DCWF basic-level courses for the workforce role 671, "System Testing and Evaluation Specialist," depicted in Figure A-2.



Source: Warfighting Acquisition University

Figure A-2. Proposed WU Courses for the System Testing and Evaluation Specialist DCWF Role

In the descriptions below, one person may fill more than one role, but each role brings a unique focus area. Government testing organizations may or may not already employ all the roles needed to support the variety of systems that the organization tests. If a government testing organization has a gap in the required cyber DT&E expertise to support testing, then it may be possible to address the gap through partnerships or contracts with other organizations. The program manager, CDT, T&E lead, and cyber lead may consider the following options to identify the desired CyWG and cyber DT&E expertise:

- Consult with similar projects, programs, and/or program executive offices.
- Borrow or establish agreements for skilled staff from similar systems' test organizations.
- Send staff for training with similar projects, programs, and test organizations.
- Fund Systems Engineering and Technical Assistance (SETA) contractors to fill in gaps (independent from the system developer).
- Resource FFRDC and/or UARC staff to fill critical CyWG roles.

Workforce Training Resources

- WU cybersecurity training (https://www.dau.edu/cybersecurity/training).
- DCWF (https://public.cyber.mil/wid/dcwf/).
- WU DCWF Cybersecurity Playlists (https://www.dau.edu/cybersecurity/cyber-playlist).
- DCWF Qualification Matrices (in accordance with DoDM 8140.03) (https://cyber.mil/cw/cwmp/qualifications-matrices/).
- National Initiative for Cybersecurity Careers and Studies Education and Training Catalog (https://niccs.us-cert.gov/training): Hosted by the Department of Homeland Security, the catalog provides more than 3,000 cybersecurity and cybersecurity-related training courses.
- CISA Learning Management System (https://niccs.cisa.gov/training/cisa-learning): Replaced the Federal Virtual Training Environment (FedVTE) and multiple other platforms to offer many of the same no cost online cybersecurity training.
- Cybrary (https://www.cybrary.it/catalog/): Provides free and fee-based cybersecurity training on a variety of popular topics.

A.2.1 Chief Developmental Tester or Test and Evaluation Lead

The program manager should staff a project with a CDT or T&E lead, optimally with a cyber test background. Before selecting personnel to support testing, the CDT or T&E lead should understand the expected system design, system technologies, and system interfaces. The CDT or T&E lead can work with the engineering team to first understand the system's design and then determine the skills needed to test the system and include them in the list of cyber DT&E personnel. The system design, though undetermined initially, is the primary driver for selecting skilled personnel to perform testing and to inform test scheduling, tool, and infrastructure planning (see Appendix J:) and the threat characterization (see Appendix D:). Eventually, the system developer, once under contract, should participate in the CyWG and help with refining the desired test expertise as the design specifics emerge.

A.2.2 Cyber DT&E Leads

The LDTO or the lead cyber DT&E organization should provide a cyber DT&E lead to the CyWG who will work closely with the cyber analyst(s) to develop the DT&E roadmap of system developer and government cyber DT&E events, including the government cyber acceptance T&E needed to evaluate the system's functional cyber performance requirements. The cyber DT&E lead should plan government cyber DT&E events, recruit the staff needed to support the events, develop test plans, and document test results in reports. The cyber DT&E lead and the cyber analyst(s) should observe system developer test events, if possible, and review the detailed

system developer test results to provide the CDT or T&E lead with a technical analysis of the test and findings.

For each system developer or government cyber DT&E event using a test range or test lab, a cyber DT&E event lead (system developer, government, range) is responsible for leading the test team executing each event. The cyber DT&E lead and the cyber DT&E event lead work together in executing all DT events.

The DoW CyberDT XSWG recommended a set of qualification standards expressed as knowledge, skills, and abilities for cyber DT&E leads, including technical and leadership skills. For more information, refer to the Developmental Test Cyber Vulnerability Analysis Standards (https://go.intelink.gov/workforce).

The DCWF workforce role knowledge, skills, and abilities for "System Testing and Evaluation Specialist," "AI Test & Evaluation Specialist," and "Software Test & Evaluation Specialist" may be appropriate for the cyber DT&E lead.

A.2.3 Cyber DT&E Technical Experts

The term cyber DT&E technical experts is a broad description of a class of experts specializing in analyzing, planning, and conducting cyber DT&E activities. They include hands-on test teams, analysts, assessors, and SMEs in a variety of technical disciplines. The DCWF (in accordance with DoDD 8140.01, DoDI 8140.02, and DoDM 8140.03) specifies the following T&E-relevant roles that the CyWG should consider when defining the desired knowledge, skills, and abilities for the system development:

- Exploitation Analyst, Work Role ID: 121.
- Systems Security Analyst, Work Role ID: 461.
- Cyber Defense Infrastructure Support Specialist, Work Role ID: 521.
- Vulnerability Assessment Analyst, Work Role ID: 541.
- Software Developer, Work Role ID: 621.
- Information Systems Security Developer, Work Role ID: 631.
- Systems Developer, Work Role ID: 632.
- System Testing and Evaluation Specialist, Work Role ID: 671.
- AI Test & Evaluation Specialist, Work Role ID: 672.
- Software Test & Evaluation Specialist, Work Role ID: 673.

WU is coordinating with the DoW CIO to deliver courses enabling various DCWF workforce roles.

A.2.4 Cyber Analysts

The role of cyber analyst may align to several different cyber roles, based on the program manager's organization support structures in accordance with DoDI 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements." The DCWF contains more information on cyber analyst roles. Cyber analysts examine architectures, controls, countermeasures, requirements, threats, and the functional system and develop a view of the system's security posture as the subject of testing. They consider assessment methods that are appropriate for the system and ensure that the chosen assessments align to the test objectives. The SUT may be a subcomponent, subsystem, component, software, integrated components or architectures, or networks and protocols. The cyber analyst assists in planning all cyber DT&E using STAT to design a continuum of testing maturing with system development and reduces risk while assessing operational resilience and system cyber resilience. The cyber analyst helps ensure the correct scope of testing and the timing and frequency of testing while assisting the CDT or T&E lead with selecting the SMEs and other experts described in this appendix. The cyber analyst assists in ensuring that the TEMP or T&E strategy accurately reflects the testing, resources, and schedule for cyber DT&E activities. Cyber analysts support:

- Analyzing cybersecurity requirements and characterizing the attack surface.
- Planning and conducting MBCRAs.
- Defining the scope of the government cyber DT&E events and assessing the level of effort required to support and complete the cyber DT&E.
- Assisting the CyWG in capturing cyber DT&E event objectives for government and system developer testing.
- Proposing the scope of system developer cyber DT&E events to support government test objectives.
- Supporting DoW RMF security controls assessment.



- Coordinating with the respective stakeholders for formal approval.
- Working with the CyWG to ensure that the classification level of repositories, events, test tools, environments, data, and reports aligns with the SCG and that authorized individuals can access the information.
- Identifying the cyber DT&E events that are appropriate to indicate in the IDSK (see Section K.2.7).

- 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.

Cyber Analysts – Recommended Minimum Qualifications

The WU Cyber T&E Foundational Credential should enable cyber analysts to provide the support described above. Cyber analysts should have the following qualifications:

- Knowledge of:
  - The organization's:
    - Enterprise information security architecture system.
    - Evaluation and validation requirements.
    - Threat environment.
  - Network protocols (e.g., Transmission Control Protocol (TCP)/IP, Dynamic Host Configuration Protocol) and directory services (e.g., Domain Name System (DNS)).
  - Network hardware devices and functions.
  - Systems administration concepts.
  - The SE process.
  - Penetration testing principles, tools, and techniques.
- Familiarity with common tools that attackers use.
- Experience with offensive security analysis tools and tactics.
- Experience in:
  - Designing a data analysis structure (i.e., the types of data that the test should generate and how to analyze the data).
  - Determining an appropriate level of test rigor for a given system.
  - Developing operations-based testing scenarios.
  - Testing systems integration.
  - Writing test plans.

As previously stated, if cyber analysts with the necessary knowledge and skills are not part of the system development, the program manager should seek supplemental support from either

contractor service support, FFRDCs, UARCs, or the testing organizations supporting cyber DT&E.

A.2.5 Other Subject Matter Experts

A.2.5.1 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. See the CUI Appendix L for additional considerations when testing specialized assets. The program manager's organization should select cybersecurity SMEs with skills aligning with the major design components of the system. In addition, the CyWG should ensure the availability of relevant SMEs for specific COTS or government off-the-shelf (GOTS) testing. The SMEs should support the planning and analysis activities to scope the testing events and should participate when the testing for their specialty area or component is in scope.

A.2.5.2 Intelligence Subject Matter Experts

Intelligence SMEs provide expertise on the tactics of the threat adversary used during testing. Intelligence SMEs, with respect to cyber, understand the full suite of attack vectors and can help test teams focus system tests on the key cyber terrain that adversaries may target. These SMEs inform *Planning for Cyber DT&E* events.

A.2.5.3 Operational Subject Matter Experts

Operational SMEs help cyber test teams understand how the system functions. SMEs may come from acquisition program offices, intelligence, military personnel, OTAs/OTOs, research and development (R&D) organizations, system developers, 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.

A.2.5.4 Software Assurance Testing Subject Matter Experts

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

A.2.5.5 Hardware Assurance Testing Subject Matter Experts

Hardware assurance testing SMEs specialize in designing, developing, and executing comprehensive testing methodologies to validate the security, integrity, and functionality of

hardware components and systems, including activities such as vulnerability assessment, penetration testing, and reverse engineering to identify and mitigate potential threats and weaknesses.

A.2.5.6 System Security Engineering Subject Matter Experts

SSE SMEs specialize in crucial SSE disciplines (i.e., software and hardware assurance, SCRM, AT, and defense exportability features). The SMEs can assess related testing requirements and recommend appropriate tools, methods, and resources needed to properly evaluate and test for relevant program protection requirements.

Other Subject Matter Experts – Recommended Minimum Qualifications

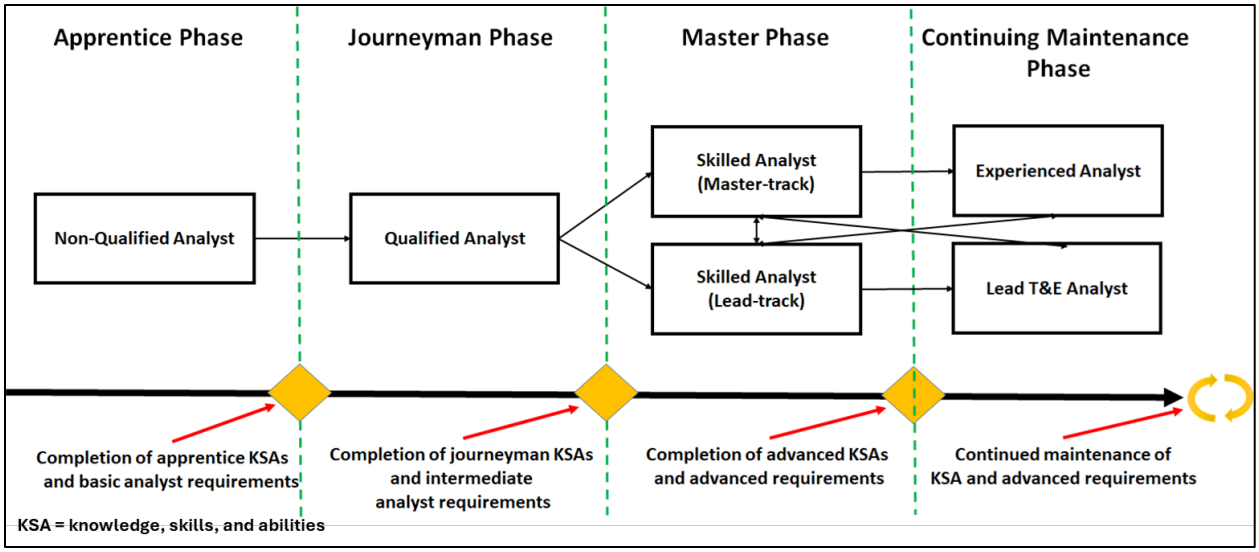
The SMEs and qualifications needed will vary from system to system and test to test. The CyWG should select SMEs with the credentials and experience to support the test design and execution based on the design components of the system.

A.2.6 Cybersecurity Vulnerability Analysts

Cybersecurity vulnerability analysts (VAs) are hands-on test personnel who use both automated tools and manual techniques to look for known vulnerabilities and attempt to exploit the vulnerabilities to understand the likelihood and impact of the exposure. Typically, they are experts on STIGs for COTS and GOTS, and they often function as both security controls assessors and vulnerability assessors. Cybersecurity VAs support test activities and should participate in the CyWG. Cybersecurity VAs may provide test data and characterize deficiencies for root cause determination to identify corrective actions. The DCWF workforce role knowledge, skills, and abilities for "Vulnerability Assessment Analyst" are also appropriate for this role.

Cybersecurity Vulnerability Analysts – Recommended Minimum Qualifications

The knowledge and recommended qualifications for cybersecurity VA hands-on test personnel vary in terms of the protocols, architectures, and networks in the scope for testing. The DoW CyberDT XSWG recommended a set of knowledge, skills, and abilities and a progression of knowledge for cybersecurity VAs. The standards allow organizations to train and develop their workforce to support cyber DT&E events and may include complementary requirements. Different proficiency levels are beneficial, and the cybersecurity VA standards describe a career progression from apprentice to master VA and lead VA. Figure A-3 shows this progression. For more information, refer to the Developmental Test Cyber Vulnerability Analysis Standards (https://go.intelink.gov/workforce).



Source: Cyber Developmental Test Cross Service Working Group Vulnerability Analysis Standards

Figure A-3. Vulnerability Analyst Proficiency and Maturity Levels

A.2.7 Penetration and Adversarial Test Teams

Penetration and adversarial test teams (PATTs) or DCATs are test teams who specialize in testing using exploits and adversary tactics. Some T&E communities also refer to PATTs and DCATs as red teams. However, not all DCATs are DCRTs as defined in DoDI 8585.01, "DoD Cyber Red Teams," and described in Section A.2.8 of this appendix. PATTs should be engaged with the CyWG when available beginning in the initial *Iterative Planning for Cyber DT&E* and to support MBCRAs. The CDT or T&E lead should expect a PATT to be performing the testing. The DCWF does not include a specific role with knowledge, skills, and abilities directly aligned to a PATT.

Penetration and Adversarial Test Teams – Recommended Minimum Qualifications

PATTs selected to conduct testing for a system should have prior experience with the protocols, architectures, networks, and interfaces associated with the SUTs. The basic skillsets expected of a penetration tester include:

- At least 3 years of related cybersecurity experience.
- Familiarity and experience with common operating system environments.
- Familiarity with:
  - Common tools that attackers use.
  - TTPs that attackers use.

  - Cybersecurity defenses (intrusion prevention systems, intrusion detection systems, firewalls, security information and event management, etc.).
- Experience with offensive security analysis tools and tactics.
- Experience performing open-source research.
- Experience analyzing data from various sources of information and identifying potential vulnerabilities and attack vectors.
- Proficiency in scripting languages (such as Python, Perl, or Ruby).
- Operational understanding of TCP/IP and computer networking.

A.2.8 DoW Cyber Red Teams

DCRTs are certified by NSA and accredited by the U.S. Cyber Command to conduct cyber operations across the DoD Information Network (DoDIN) in support of and as authorized by the appropriate DoW Component, DoDIN area of operations commanders, DoDIN area of operations directors, and AOs for the relevant cyber terrain. DCRTs conduct adversarial cyber tests of or through a system, service, or enclave exploiting identified vulnerabilities and other weaknesses in coordination with an OTA, DT&E organization, or the program management office. While engaged, DCRTs can conduct actions openly and in collaboration with the system or mission owners using threat-based capabilities and rigorous methodologies to assess systems under acquisition, enclaves, and networks in a mission-relevant threat environment. DCRTs create operational effects through the identification and exploitation of vulnerabilities in systems under acquisition testing. Cyber DT&E requires a DCRT only when crossing authorization boundaries. This situation occurs when a developmental SUT operating with a valid ATO or interim authority to test interacts with deployed or operational systems operating under an ATO.

DoW Cyber Red Teams – Recommended Minimum Qualifications

The DCRT should have prior experience with the protocols, architectures, networks, and interfaces associated with the SUTs and possess a current NSA red team certification and U.S. Cyber Command accreditation to conduct cyber operations across the DoDIN. Refer to DoDI 8585.01 for additional information on DCRTs.

A.2.9 Cyber Test Range Representatives

Cyber test range representatives assist the CyWG in planning the test environments and test infrastructure needed to conduct cyber DT&E. They have specialized technical knowledge and experience in building test environments. Cyber test range representatives possess analysis and test skills in the areas of penetration testing and adversarial testing to support cyber DT&E

planning. These skills include knowledge of distributed testing; virtual environment emulation; network engineering; adversary access methods and tactics; and intelligence to generate effective range capabilities, characteristics, and scenarios. Cyber test range representatives may include the following roles needed to plan and conduct cyber DT&E 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.
- 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 the adequacy of bandwidth between distributed sites; the 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.
- 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.
- Security engineer: Personnel who monitor, manage, and configure security devices and controls associated with cyber range events.

Cyber Test Range Representatives – Recommended Minimum Qualifications

The cyber test range representative should bring specific knowledge of the requirements for high-fidelity, representative contested cyber environments to conduct cyber DT&E during all phases of the system life cycle and testing of complex SoS. If needed, NCRC SMEs are available through the Test Resource Management Center (TRMC) to support the planning, execution, and analysis of test and training events. TRMC may further leverage available expertise from the Department of Energy, national laboratories, and other sources as necessary and appropriate. Personnel fulfilling this role should have the following skills:

- Knowledge and understanding of the use of live, virtual, constructive, and distributed environments for the conduct of cyber DT&E.
- Knowledge and ability to design, deploy, and sanitize large-scale, high-fidelity test and training environments in allowing the release of malicious threats on operationally representative systems and networks to assess their impact.
- Knowledge of:
    - The NCRC and other DoW cyber ranges and methods to collaborate test environments across the cyber ranges using secure networks.

- DoW test range capabilities and facilities and awareness of other T&E facilities and resources within and outside DoW.

A.2.10 System Developer Staff

System developer staff are frequently the experts for the government systems they are building and therefore should be members of the CyWG. They supplement the knowledge of government design and test teams.

System Developer Staff – Recommended Minimum Qualifications

System developer staff should have the following qualifications:

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

A.2.11 Security Champion

The security champion is a member of the product team and CyWG and assists in improving the communication between the development teams, engineers, cybersecurity team, and CyWG. Security champions represent the developers to the CyWG. Additionally, security champions will usually be involved in risk/threat assessments and architectural reviews and can often help identify opportunities to remediate security defects, making the architecture of the application more resilient and reducing the attack threat surface. Security champions also participate in periodic briefings to increase awareness and expertise in different security disciplines. Finally, the security champion promotes and tracks secure coding practices and ensures that security is a constant consideration in processes and tools. A security champion does not have to be a security

professional but should have a strong interest in security and a desire to learn more about security.

Security Champion – Recommended Minimum Qualifications

The security champion should understand the challenges faced by DevSecOps engineers. The security champion should have strong interpersonal skills and be a good communicator. Although not required, the security champion may benefit from earning cybersecurity certifications or attending technical cybersecurity training.

Desired qualifications for the security champion include knowledge of:

- Cybersecurity and cyber resilience best practices.
- Secure coding practices, network security, and incident response.
- The organization's overall security posture and the specific security risks and challenges that the organization faces.
- Cybersecurity current events.
- Security standards and procedures.
- DevSecOps, developer best practices, and system development.

The security champion's role may also involve:

- Understanding cyber adversarial threats and threat models.
- Performing code reviews.
- Conducting or verifying automated security scanning and tools.
- Prioritizing security fixes.
- Tracking security backlog items and system deficiencies.
- Providing support to cyber DT&E test teams.

A.3 Cyber Working Group

The program manager will charter a CyWG in accordance with DoWM 5000.103 at the initiation of the research or pre-acquisition project, the initiation of an acquisition program, or before any contractual commitment or release of the first RFP. The CyWG is responsible for advising the program manager and CDT or T&E lead on the full range of cyber DT&E activities to verify the cyber performance requirements for the system. The CyWG should ensure that it has the right collaborative team members and the right skills from the system developer, program manager's

organization, and government DT&E organizations to perform the activities and tasks of *Iterative Planning for Cyber DT&E*.

The roles and personnel detailed in Table A-1 are potential members of the CyWG. Not every role will fit for every acquisition and for the size and complexity of the CyWG scoped to the SUT and the requirements under test.

In accordance with DoWM 5000.103, the chartered CyWG observes and tracks the progress of system developer cyber T&E to ensure consistency with the TEMP or T&E strategy and determines the priorities for cyber DT&E. (DoWM 5000.103 contains the detailed set of CyWG responsibilities.)

A.3.1 CyWG Participants and Roles

Table A-1 lists the recommended CyWG participants and summarizes their roles.

Table A-1. CyWG Participant Roles

Recommended CyWG Participant	Role
Anti-Tamper (AT) Representative	Provides insights and advice on the information and testing required to attain AT requirements and potential implications such as constraints on testing from such requirements.
CDT, T&E Lead, or SSE Lead	Manages all DT&E activities.
Cyber DT&E and OTA/OTO Technical Expert (test team/analyst/assessor)	• Supports test design and execution based on the design components of the system. • Ensures the availability of relevant SMEs for specific commercial off-the-shelf or government off-the-shelf testing.
Cyber SME	Advises based on their subject matter expertise in support of cyber T&E.
Cyber Test Range Representative	Provides insights and advice on the available capabilities and proper use of cyber ranges and assists with the processes for gaining access to and scheduling these resources.
Cyber Test/Analyst Team	Cyber Analysts: • Are the backbone of an organization's cyber program. • Within the CyWG, they primarily develop a holistic picture of a SUT's security posture and cyber capabilities by examining the SUT functions, architectures, controls, countermeasures, requirements, threats, test data and reports, contract documents and deliverables, the ICT supply chain, etc. • May be government civilians, military personnel, FFRDC personnel, UARC personnel, or Systems Engineering and Technical Assistance (SETA) contractors. Cyber Test/Analyst Team:

Recommended CyWG Participant	Role

	• Analyzes cyber requirements and provides input to contract documents.
	• Conducts attack surface characterization.
	• Plans and supports MBCRA events. (Appendix G:.)
	• Assists with development of the cyber T&E input for the TEMP or T&E strategy:
	  – Test objectives, resources, and schedule.
	  – Scope, frequency, and timing of government cyber test events.
	  – Prioritization of SUTs.
	• Works with scientific test and analysis techniques (STAT) experts to design a continuum of testing that matures with system development.
	• Identifies and scopes the resources and budget required to plan and perform cyber test events:
	  – Technical experts, cyber SMEs, test articles, tools, infrastructure, etc.
	• Provides input for cyber evaluations.
	• Proposes the scope of system developer cyber testing events to support government test objectives.
	• Supports DoW RMF security controls assessment.
	• Coordinates with the respective stakeholders for formal approval of cyber documents.
	• Works with the CyWG team to handle cyber T&E event and report data at the appropriate level if defined in a security classification guide.
	• May include SETA contractors.

Cyber-Intelligence SME	• Ensures the availability of current threat intelligence and pursues requests for information to enable the CyWG activities. • Provides expertise on the tactics of the threat adversary used during testing. • Understands the full suite of attack vectors. • Helps test teams focus system tests on key cyber terrain that adversaries may target. • Plans for adversarial test activities.
Cybersecurity Service Provider (CSSP) and Defensive Cyberspace Operations (DCO) Representative	• Provides insight on the ability of the CSSP and DCO personnel to integrate the system into existing cyber defenses and tools. • Coordinates participation of the CSSP and DCO personnel for tests and other cyber activities.
Engineering Discipline: Lead Systems Engineer Representative, SSE or SE Lead	A systems engineer in DoW develops, designs, allocates, and manages the SUT to adhere to user and system-level requirements. • Leads development of the system architecture.

Recommended CyWG Participant	Role
	• Evaluates design trade-offs; balances technical risk between systems. • Defines and assesses interfaces. • Provides oversight of verification and validation activities. • Conducts many other tasks throughout the course of system development.
Information Security System Manager 	• Is responsible for the cybersecurity risk assessment of a program, organization, system, or enclave. • Applies cybersecurity risk management and synchronization of the DoW RMF process with the system's life cycle processes in accordance with DoDI 8510.01.
Interoperability Representative and Test Team	Provides insights and advice on the requirements, data needs, and testing for interoperability including identifying tests to provide the needed data and maintaining the status of interoperability testing.
Lead DT&E Organization Representative	Represents the government T&E organization that is responsible to the T&E lead for guiding DT&E throughout the acquisition process to assist in engineering design and development and to verify that the system meets technical performance specifications.
Lead Software Engineer/Architect	Leads the design, development, testing, and maintenance of software applications.
Modeling and Simulation (M&S) SME	Provides insights and advice on the capabilities, limitations, status, and use of available and applicable M&S and on the verification, validation, and accreditation requirements, plans, and status for the M&S.
Operational SME	Provides context for the warfighter capabilities that the system supports.
OTA/OTO Representative	• Advises and coordinates on the activities, data, and resources needed for the OTA/OTO to independently plan, conduct, and report on the cyber OT&E for the acquisition program. • Co-chairs the integrated test team and CyWG with the CDT or T&E lead or another designee.
Oversight Organization and Other Relevant Stakeholder	Includes representatives from the oversight organizations, consistent with the specific oversight list.
Security Champion (DevSecOps)	• Serves as the liaison between developer teams and cyber T&E. • Ensures that developers consider security, follow secure coding practices, and understand cyberspace threats to software development and software supply chains.
Security Control Assessor 	Provides advice, coordinates activities, and ensures the sharing of information between the security controls assessment activities and cyber T&E.

Recommended CyWG Participant	Role
Service-Specific T&E Policy Representative	Provides insight and advice on how existing policy could affect the proposed CyWG activities.
Software Assurance Testing SME	• Provides insights from completed software assurance testing and advises on how CyWG activities can inform and support software assurance. • Specializes in testing software at the code level. • Examines code for code-based vulnerabilities. • Recommends test tools specific to software testing such as static and dynamic test tools.
STAT and Design of Experiments SME	Provides insights and advice on statistical techniques to inform the planning, evaluation, and reporting of results.
SUT System Developer and Test Team	Designs, develops, tests, and evaluates (information) systems throughout the system development life cycle.
System Maintainer and Logistician	Provides insight and advice on cyber supply chain and maintenance considerations for the system.
System Operator	• Operates the system in the operational environment. • Helps cyber test teams understand how to use the system and how the system functions.

A.3.2 Establishing CyWG Roles and Responsibilities

As discussed in Section 2 of this guidebook, a chartered CyWG ensures the accomplishment of the cyber DT&E activities. The CyWG is a cross-organizational and cross-functional group. One method to manage the roles and responsibilities for planning and conducting cyber DT&E is to build a "Responsible, Accountable, Consulted, and Informed" (RACI) matrix listing the various personnel and their appropriate RACI assignment for each task. Figure A-4 is an example RACI matrix.

The original RACI example matrix is available in Microsoft Excel on https://go.intelink.gov/Cyber_DTE.

Responsible (R): The person or people who do the work to complete the task.
Accountable (A): The person who is ultimately answerable for the completion of the task and has the authority to approve or reject the work.
Consulted (C): The person or people who provide input or expertise before the task is completed.
Informed (I): The person or people who are kept informed of the progress or completion of the task, but are not actively involved in its execution.

Cyber T&E Stakeholders → / Cyber DT&E Activities and Tasks	Program Manager or Equivalent	CDT	Systems Security Engineer	ISSM	Lead Software Engineer/Analyst	System Developers	Lead D&TE Organization	OTA/OTO	Cyber DT&E and OTA/OTO Technical Experts	Security Controls Assessor	Cyber SME	Cyber-Intelligence SME	CSSP	System Maintainer and Logistics	Cyber Test Range	Service-specific T&E Policy Representative	Approving Official	Software Assurance Testing SME	Security Champion (DevSecOps)	STAT and Design of Experiments SME	M&S SME	Anti Tamper	System Operators	Operational SME	Oversight Organizations	Other Relevant Stakeholders
	RACI																									
Identify cybersecurity lead	R-A	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Designate LDTO	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Establish and charter the cyber working group; include any specialized cyber expertise to support the T&E WIPT, SSEWG, and any other IPT and/or WIPT as appropriate	R-A	C	C	C	C	C	C	C	I	I	C	C	I	C	I	I	I	C	C	I	C	I	C	C	I	I
Include cyber DT&E requirements in each RFP and contract (e.g., system developer, etc.)	A	R	R	C	C	I	C	C	I	I	R	C	I	C	I	I	I	C	C	I	C	I	C	C	I	I
Examine and advise on cyber requirements	R-A	C	R	C	C	I	C	C	I	I	R	C	I	C	I	I	I	C	C	I	C	I	R	R	I	I
Review relevant documentation at the initiation of the project or acquisition program and recurringly throughout the system's life cycle.	A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	I	R	R	R	R	R	R	R	C	I
Examine current threat assessments	A	A	R	R	I	I	R	R	I	I	R	A	I	I	I	I	R	I	I	I	I	I	I	R	I	I
Characterize cyber attack surface	A	I	R	C	C	R	I	I	I	I	R	C	C	C	C	I	I	I	C	C	C	C	C	C	I	I
Support criticality, vulnerability, supply chain, and mission-relevant terrain in cyberspace analysis	A	I	R	C	R	R	I	I	I	I	R	R	C	R	C	I	I	I	C	C	C	C	R	R	I	I
Develop or update all applicable cyber DT&E sections of TEMP or T&E Strategy (e.g., MBCRA, IDSK)	A	R	R	R	C	R	C	C	I	I	R	R	I	C	I	C	I	C	C	C	C	C	I	I	C	I
Confirm cyber T&E informs S&T approach or program's acquisition strategy, cybersecurity strategy, engineering plans, and other plans.	A	R	R	R	C	I	C	C	I	I	C	C	I	C	I	C	I	C	C	C	C	C	I	I	C	I
Conduct or update MBCRA	A	R	C	C	C	C	C	C	C	I	C	C	C	C	I	I	I	C	C	C	C	C	C	C	C	C
Plan resources and schedule government DT&E	A	R	I	I	I	C	C	C	C	I	I	C	I	C	C	I	I	I	I	I	I	I	I	I	C	I
Plan, fund, and maintain test infrastructure, cyber ranges, test articles, tools, and data requirements	A	R	I	C	I	C	R	R	R	I	I	I	I	R	C	I	R	R	R	I	I	I	I	I	I	I
Confirm integration of the DoD RMF and cyber T&E processes	A	R	I	R	I	R	C	I	C	R	I	I	I	I	I	I	A	I	I	I	I	I	I	I	I	I
Integrate all available prior cyber or non-cyber test results into SSE and test planning; ensure data availability for subsequent testing and to verify mitigations	A	R	R	R	C	R	R	R	C	I	C	C	I	C	I	I	I	C	C	I	C	C	I	I	I	I
Provide resources and confirm schedules	A	R	I	C	I	R	R	R	C	I	I	C	I	C	R	I	I	I	I	I	I	I	I	I	C	I
Gather, Develop, and Approve Detailed Cyber DT&E Plans	A	R	C	C	C	R	R	R	C	I	C	C	I	C	C	I	I	C	C	C	C	C	I	I	I	I
Verify products are compliant with STIGs and analyze exposures to known vulnerabilities	A	R	C	R	I	R	R	R	I	C	C	I	I	I	I	I	C	I	I	I	I	I	I	I	I	I
Review system developer cyber DT&E strategy and all test plans as received	A	R	R	R	C	R	R	R	C	I	C	C	I	C	I	I	I	C	C	R	C	C	I	I	I	I
Conduct Cyber DT&E Test Readiness Reviews	A	R	I	R	I	R	R	R	R	I	R	I	I	I	R	I	I	R	R	R	I	R	C	R	I	I
Prepare for Cyber DT&E Events	A	R	I	I	C	R	R	R	C	I	I	I	I	I	R	I	I	I	I	R	I	I	I	I	I	I
Obtain IATT, ATO, ATC, ISA, and/or complete RMF assessment as necessary	A	R	C	R	C	I	I	I	I	R	C	I	I	I	I	I	R	C	C	I	I	I	I	I	I	I
Employ real or simulated operational interfaces to inform joint interoperability certification, as necessary	A	R	C	I	C	R	R	R	C	I	C	I	I	I	I	I	I	I	I	I	R	I	I	I	I	I
Execute security verification throughout the system's life cycle	A	R	C	R	C	R	R	R	I	R	C	C	C	C	I	I	I	C	C	I	I	C	I	I	I	I
Execute planned system developer or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system	A	R	C	C	C	R	C	C	R	I	C	C	C	C	R	I	I	R	C	C	C	R	I	I	I	I
Execute planned government acceptance cyber T&E	A	R	C	C	C	C	R	R	R	I	C	C	C	C	R	I	I	R	C	C	C	R	I	I	I	I
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events	A	R	C	C	C	C	R	R	R	I	C	C	C	C	R	I	I	R	C	C	C	R	I	I	I	I
Review cyber test results, as received, and plans for consistency with the TEMP or T&E strategy, remediation and regression testing, and recommend mitigation strategies	A	R	C	C	C	R	R	R	R	C	C	I	I	C	R	I	I	R	C	I	I	R	I	I	I	I
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones	A	R	C	R	I	R	R	R	R	R	C	I	I	I	I	I	C	I	I	R	I	R	I	I	I	I
Report on cyber DT&E activities and deficiencies (e.g., JDRS); maintain and make available all documentation, artifacts, T&E data, and system developer reports available to authorized users	A	R	I	R	I	R	R	R	R	I	I	I	I	I	R	I	I	R	I	R	I	R	I	I	I	I
Update cyber DT&E strategy in TEMP or T&E Strategy	A	R	R	R	C	R	C	C	I	I	R	R	I	C	I	C	I	C	C	C	C	C	I	I	C	I

Figure A-4. Example RACI Matrix

A.4 Maintaining Cyber DT&E Proficiency

The DoW CyberDT XSWG recommended a set of organizational standards to assess whether cyber DT&E organizations possess the administrative capability to support events; possess highly qualified cybersecurity VA personnel; and show commitment to the development and retention of their workforce. These standards ensure that organizations can perform cyber vulnerability assessments and analyses across cyber DT&E execution. Table A-2 summarizes the organizational qualification standards to support cyber DT&E.

Table A-2. Organizational Cyber DT&E Standards

Organizational Standard	Description
Professional Development	The organization possesses a funding line to provide formal training; develops and maintains in-house training specialized and targeted to customer mission space; has the capability for participation in R&D/S&T innovation projects to support cyber vulnerability analysis and assessments; is an active participant in joint cybersecurity VA training exercises; and provides cyber subject matter expert (SME) workforce career advancement opportunities for formal education, TEMP or T&E strategy assignment rotations, and the Warfighting Acquisition University.
Cybersecurity Vulnerability Analyst (VA) Tools	The organization has the resources and capacity to develop custom mission-based VA tools, techniques, and methodologies; configuration management processes, procedures, and infrastructure for VA tools; and appropriate documentation for the use of developed 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 cyber DT&E mission/technology to facilitate professional development.
Human Capital	The organization has processes and procedures as part of its hiring plan to hire qualified cyber SMEs and provides opportunities to incentivize and retain its cyber workforce.
Procurement	The organization has a funding line to procure equipment and services to support cyber DT&E workforce maintenance and development.
Work Products Standards (Test Plan)	The organization has the capacity to staff test plans in support of VA events. The organization should provide a test plan containing (but not limited to) the following required sections: rules of engagement (ROE), VA methodology and tools, system characterization, characterized attack surface and attack vectors, and event constraints and limitations.
Work Product Standards (Final Report)	The organization has the capacity to staff VA technical reports and ensure that the report includes the following required information: evidence of confirmed cyber vulnerabilities, VA risk assessment mitigation, and risk management recommendations.
Legal Review Process	The organization has an internal legal review process to cover the approval of all (standard) test plans, standard operating procedures, and ROE and respond to test-critical questions or issues within 48 hours for any VA event.
Threat Intelligence	The organization has established relationships with the threat intelligence community including organizations that provide current threat information and participation in working groups biannually at a minimum.

Organizational Standard	Description
Community Relationship	
Standard Operating Procedures	The organization possesses a baseline set of standard operating procedures in support of cyber DT&E ensuring that the organization conducts effective planning, execution, and post-analysis of VA events (e.g., emergency halting procedures).

A.5 Cyber DT&E Staffing in the TEMP or T&E Strategy

The TEMP or T&E strategy should describe the personnel resources needed to support the cyber DT&E test strategy including the personnel required for cyber analysis, testing, and assessments. It should include a brief description of the CyWG and the cyber DT&E roles and responsibilities. There should be a high-level summary of the personnel resources needed to execute cyber DT&E; resources should be in alignment with the T&E budget exhibits (Acquisition Category I programs). These elements include funding and workforce for test conduct and support (cybersecurity teams, SMEs, additional test teams, data collectors, trusted agents, etc.). The CyWG should ensure cyber DT&E resources provided by the system developer are detailed in either the development or production contract. (See Appendix I:.)

A.6 Cyber DT&E Organizations

For a current list of T&E organizations and cyber test ranges, refer to the Service Providers and Facilities under the Cyber T&E group on JETEP (https://jetep.apps.dso.mil/). Figure A-5 shows Cyber T&E as an option on the JETEP Website. To create a Platform One (P1) account:

1. Visit the Registration Page (https://login.dso.mil/register).
2. Fill out the Registration Form.
3. For common access card (CAC)/Impact Level (IL) 4 access (required for JETEP): Use a ".mil" email address and leave the password fields blank until after account creation with a CAC.
4. Check email (and the junk folder) for the verification link and click it to complete the P1 account setup.



Figure A-5. JETEP Homepage

Appendix B: Examine and Advise on Cyber Performance Requirements and Measures for Cyber DT&E

This appendix provides considerations for how the CyWG examines and advises on functional cyber performance requirements and measures. Cyber DT&E executes verification for cybersecurity and cyber resilience requirements (expressed through architecture, standards, and implementation); substantiates achievement of contract technical performance; and certifies readiness for initial operational testing. Measurable and testable cyber requirements enable consistency, scientific test methods and techniques, and repeatability throughout the system life cycle.

To test a system, the most fundamental activity is to stimulate the system under a controlled environment and compare the expected response to the actual response. DoW has a long history of testing and evaluating system performance and system reliability; however, assessing cybersecurity and cyber resilience in a representative contested cyber environment is challenging because of the nature of the computational state space. Evaluating a system's cybersecurity and cyber resilience differs in the deterministic nature of cyber devices (e.g., running the same test with the same inputs multiple times should result in the same output; for the system to perform differently, a change in the environment or the system likely occurred). This appendix addresses the understanding of the measures and methods to test and evaluate the differences.

B.1 Characteristics of Cyber Requirements

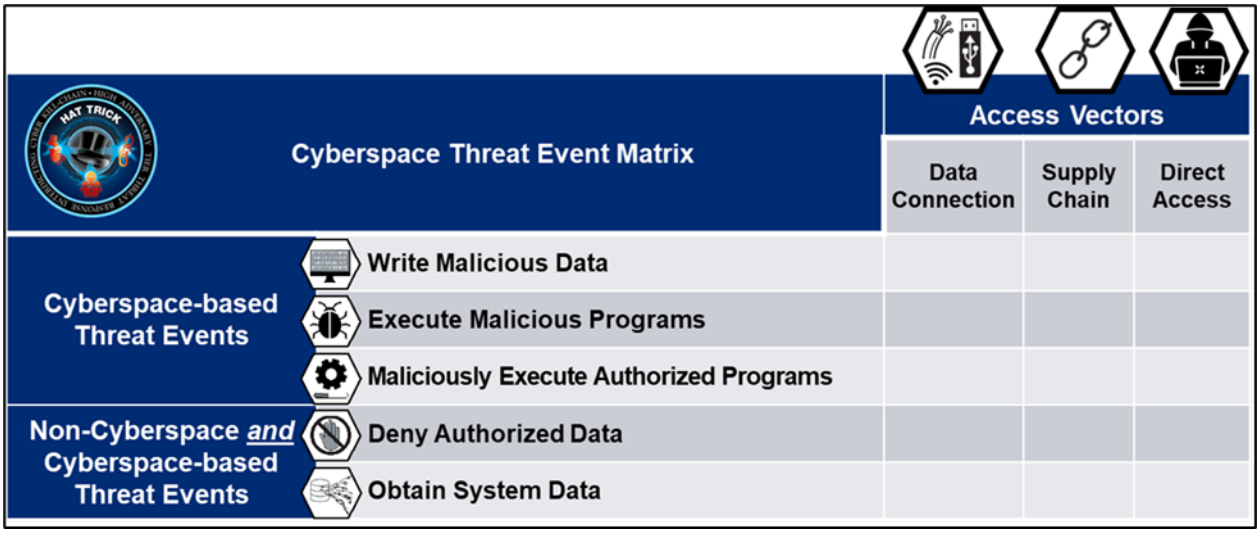
This section uses "types" and "categories" in the following paragraphs as descriptions, not to prescribe definitions. WU and the International Council on Systems Engineering (INCOSE) provide extensive guidance on "good" requirements and systems engineering. For more information, see the INCOSE Systems Engineering Handbook (https://sebokwiki.org/wiki/INCOSE_Systems_Engineering_Handbook).

Cyber requirements may be in any of the following types: performance, functional, technical/ nonfunctional, or regulatory/compliance.

- **Performance requirements**. Performance requirements define the standards determining a system's effectiveness, responsiveness, and scalability. These requirements are typically less specific than functional requirements, focusing on how well a system performs rather than what it performs. In the example below, the requirement does not describe a specific behavior or capability that the system performs but rather a performance characteristic that the system possesses:
    - Example: The <detection system component> must be able to detect and quarantine an anomaly within 5 seconds of its occurrence with a probability of 0.99.

- **Functional requirements**. A functional requirement is a task (sometimes called action or activity) that a system should successfully complete to provide an operational capability (or satisfy an operational or mission requirement). Functional requirements describe the specific behaviors, capabilities, or features that a system should have to satisfy its intended purpose.
    - Example of a poor requirement: The system must be able to detect unauthorized programs within 10 milliseconds of execution without blocking critical function A or critical function B. (This requirement is not measurable and testable because it lacks detail, constraints, and restraints.)
    - Example of a better requirement: The system must be able to detect execution of unauthorized programs of type X, Y, and Z within 10 milliseconds of their resource request, while executing critical function A and critical function B, in expected environmental and load conditions (system is operating under normal conditions and when the CPU utilization is above 80 percent).
- **System technical or nonfunctional requirements**. System technical requirements (typically allocated or derived from other requirements) refer to the specific hardware, software, and network configurations necessary for a particular system or software application to function optimally.
    - Example: The backplane resource monitor must be able to report detected unauthorized instructions running in memory.
- **Regulatory or compliance requirements**. DT&E is not the typical verification method for these requirements. Compliance requirements should be specific, measurable, and achievable and should focus on the most relevant and important requirements for the system. A specification is a detailed, exact statement of particulars, especially a statement prescribing materials, dimensions, and quality of work. These requirements might be better suited for the SOW rather than the system specification because system developer designs to achieve the specification may satisfy the requirement.

The matrix in Figure B-1, developed by the Johns Hopkins University Applied Physics Laboratory (JHU APL), is the High Adversary Tier Threat Response Interdicting Cyberspace Kill-Chain (HAT TRICK) cyberspace threat event matrix representing a mutually exclusive, comprehensively exhaustive set of threat events and access vectors. This matrix describes the cyberspace threat as static, enabling engineers to design the system to be resilient and defeat the threat. It does not change over time. It does not depend on intelligence. It does not matter who the adversary is or what capabilities the adversary has.



Source: Johns Hopkins University Applied Physics Laboratory

Figure B-1. HAT TRICK Cyberspace Threat Event Matrix

HAT TRICK

JHU APL documents for implementing the HAT TRICK methodology:

https://go.intelink.gov/HATTRICK

Table B-1 provides some of the example cyber requirements developed by the JHU APL HAT TRICK team that are designed to address all possible threat events. The primary goal of HAT TRICK is to enable a program management office to build new and modify existing systems today that are resilient to known and future unknown cyberspace threat events. JHU APL notes that "HAT TRICK is NOT another thing to do; it is a method to do what you already have to do."

Table B-1. High-Level HAT TRICK Requirements Examples

Requirements Examples Derived from HAT TRICK: High-Level HAT TRICK Version 6.0
Address the Cyberspace Threat Events
Write Unauthorized Data
Upon detection of unauthorized data in the <system>, the <responsible entity> must render the unauthorized data harmless within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
After unauthorized data has been rendered harmless, the <system> must restore any lost mission capability caused by the unauthorized data within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.

Requirements Examples Derived from HAT TRICK: High-Level HAT TRICK Version 6.0
Defense in Depth: Execution of Unauthorized Programs
Upon detection of an unauthorized process in the <system>, the <responsible entity> must render the unauthorized process harmless within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
After an unauthorized process has been rendered harmless, the <system> must restore any lost mission capability caused by the unauthorized process within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Defense in Depth: Unauthorized Execution of Authorized Programs
Upon detection of an unauthorized instance of an authorized process, the <responsible entity> must render the unauthorized instance of the authorized process harmless within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
After an unauthorized instance of an authorized process has been rendered harmless, the <system> must restore any lost mission capability caused by the unauthorized instance of the authorized process within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Denial of Authorized Data
Upon detection of denial of <data> required for <mission-critical function>, the <system> must communicate facts about the denial of <data> required for <mission-critical function> to a <responsible entity> within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Obtain Restricted System Data
Upon detection of unauthorized access to <restricted system data>, the <responsible entity> must remove the unauthorized access to <restricted system data> within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Upon detection of the unauthorized transfer of data from the <system>, the <system> must communicate facts about the unauthorized transfer of data from the <system> to a <responsible entity> within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Address Possible Additional Access to the System
Unauthorized Access via Data Connections
Upon detection of an unauthorized data connection in the <system>, the <responsible entity> must render the unauthorized data connection harmless within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Unauthorized Access via ICT Supply Chain in Sustainment
Upon detection of an unauthorized cyberspace asset in the <system>, the <responsible entity> must render the unauthorized cyberspace asset harmless within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Unauthorized Physical Access to Cyberspace Assets
Upon detection of unauthorized physical access to the <system>'s cyberspace assets, the <system> must communicate facts about the unauthorized physical access to the <system>'s cyberspace assets to a <responsible entity> within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.

Requirements Examples Derived from HAT TRICK: High-Level HAT TRICK Version 6.0
Defense in Depth: Unauthorized Access by Unauthorized Subjects
Upon detection of unauthorized access to the <system's cyberspace>, a <responsible entity> must remove the unauthorized access to the <system's cyberspace> within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Defense in Depth: Unauthorized Access from Authorized Subjects
Upon detection of a <system subject> accessing a <system object> for which it lacks authorization, a <responsible entity> must render the unauthorized access to <system object> harmless within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Add Type B Resilience
Defense in Depth: Detect Anomalous Behavior
The <system> must detect anomalous <system> behavior within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.
Upon detection of anomalous <system> behavior, the <system> must communicate facts about the anomalous <system> behavior to a <responsible entity> within <constraints> **[specified by sponsor]** without <restraints> **[specified by sponsor]**.

Cyber requirements may have a variety of mathematical characteristics, which will change the way the CyWG and test teams need to approach the structuring of their T&E.

The following information is adapted from the STAT Center of Excellence Report, "Scientific Test & Analysis Techniques for Software Testing." Three major categories of metrics exist for cyber-enabled systems requirements, based on their mathematical properties:

- **Qualitative**. Qualitatively measured performance requirements involve opinions about system function (e.g., "user-friendliness") and are expressed in natural language or nonnumerical forms. The requirements often describe the desired human-interface characteristics of the system or broad statements, such as "The intrusion detection system should be intuitive" or "The AI system must issue no system commands that violate safety parameters." Qualitative requirements are often subjective and require further development before using them to guide the design and implementation of the system. To evaluate the user-interface characteristics, the CyWG may employ surveys with Cranfield, Cooper-Harper, or Likert rating scales or other data collection methods with a representative set of users.
- **Continuous and stochastic**. Requirements with continuous and stochastic performance metrics are usually measures of a particular factor in terms of another, such as completion rate (e.g., calculated as a percentage) or latency (e.g., milliseconds). These requirements metrics involve continuous variables, such as time, distance, or frequency, and are subject to uncertainty or randomness. These requirements often describe the expected

performance or behavior of the system under different conditions, such as "The system must be tolerant of packet latency between 0.005 milliseconds and 500 milliseconds, with a packet loss rate of between 0 percent and 20 percent." Mathematical models of the system used for testing often use metrics for continuous and/or stochastic measurements to evaluate the performance of the system under different scenarios. For testing these requirements, design of experiments may be an appropriate choice, while maintaining the mission context of a test metric.

- **Binary and deterministic**. Binary and deterministic requirements are useful for decisions such as authentication and authorization. Decisions such as "permit/deny" or "yes/no" are not continuous measurements; therefore, the tests cannot characterize probability or likelihood. This category includes derived requirements implementing many security and functional features. These requirements involve discrete variables, such as true/false, allow/reject, on/off, or pass/fail, and are subject to strict rules or conditions. The requirements often describe the expected behavior or outcome of the system under specific conditions, such as "The system should reject unauthorized programs' write access to nonvolatile storage. While doing so, the system should execute <critical function running in memory>." Formal verification often works well for requirements with binary and deterministic metrics to ensure that the system meets its intended requirements, and then the task of the test team is to verify faithful implementation of an evaluated-good design.

These categories, in conjunction with the types of requirements (functional, performance, technical or nonfunctional, and regulatory/compliance), provide a more detailed and comprehensive view of the range of cyber requirements for a cyber-enabled system. In some cases, the qualitative requirement can lead to derived requirements that are continuous/stochastic or binary/deterministic. The use of the word "requirements" in this guidebook is not specific to these characterizations; the CyWG needs to understand the types of requirements based on the system presented and determine how to verify the requirements. The CyWG should align the verification method to the requirement. Verification methods include demonstration, examination, analysis, and test.

B.1.1 Relationship Between Requirements and Measures/Metrics

The terms measurement, metric, measure, and criterion are not identical, though some may use the terms interchangeably. The following list describes the differences between the terms:

- **Measurement**: The action or process of measuring something. It is the result of applying a metric or other method of measurement to something.
- **Metric**: A system or standard of measurement. It is a way of measuring something, often used in a specific field or discipline.

- **Measure**: A quantity or amount determined by measurement. It is a specific value obtained by using a metric or other method of measurement.
- **Criterion**: A principle or standard that test teams use to judge and evaluate results. Criteria help to make informed and objective assessments, eliminating personal bias or preferences.

The requirement includes the criterion; for example, "The system must detect unauthorized data within 3 seconds." Test teams specify measures to quantify the values supporting the criterion, such as the average number of seconds to detect unauthorized data. The team selects metrics to define the specific qualities and characteristics to measure; for example, there is no statement made about a success rate (Is 100 percent detection the goal? What if the system detects only 1 percent; is this good enough? What if the system does not detect structured query language (SQL) injection attempts but does detect buffer overflow attempts?).

- Example: Assume program leaders clarify the requirement as greater than 95 percent detection against SQL injection attempts and greater than 80 percent detection against all other fault types, within 3 seconds for each occurrence.
    - The test team can use STAT methods (see Section 2.4) to establish how many times to record the measurement in a test event for evaluation against the criteria using various tools and techniques. STAT can also highlight for leaders how many conditions were untested or that the test team could not test.
    - Before developing a test plan, the test team should consider mission context for the requirement or criterion. The test team should seek to understand what components will contribute to detecting unauthorized data and plan the testing to target those components and then seek to understand the developer's decomposition and TPMs that will demonstrate progress toward attaining the 3-second requirement for the system's critical components. Documentation may reveal that the 3-second requirement has negligible effect at the mission level, and project leaders may choose to ignore the 3-second requirement.

In general, test teams will need to select appropriate measurements to deliver evidence of requirement satisfaction. Test teams need to determine how to measure the data collected to support assessing the implementation of system attributes. For example, packet capture data are of no value without a plan to digest the data into actionable and relevant data against a requirement.

B.1.2 Relationship to Data Collection

If the test team using the SUT and instrumentation setup cannot collect the measurement (no single true source of time stamps, for example), then the test team cannot establish a value for the metric and cannot publish the measure, which makes the criterion undecided. Therefore, one large factor in verification is whether the SUT (including instrumentation) can achieve the measurement with the appropriate breadth and depth to satisfy the risk tolerance.

B.1.3 Integrated and Concurrent Cyber DT&E

As described in Sections 1.6 and 1.7, concurrent cyber and non-cyber functional testing affords an opportunity to evaluate cyber resilience, performance, and functionality while causing contested cyberspace events. For example, a requirement for "nominal operation in the face of [measures capturing a contested environment]" requires some baseline "clean-air" performance values to test against. Without concurrent testing, there is no way to distinguish the fault-condition test results from the non-fault results. Integrated system developer and government testing may be able to fulfill this need depending on the characteristics of the data collected.

The Section 3 *Iterative Planning for Cyber DT&E* and Section 4 *Preparing for Cyber DT&E* activities discuss an instrumentation approach required for measuring data. Section 6 *Evaluating Cyber Developmental Test Data* discusses the evaluation of those measurements with the associated metrics (context, mission) required to write the results, as described in Section 7 *Reporting Cyber DT&E Results*, to contribute to the data repository and inform the upcoming decisions during system development.

B.2 From Cyber Requirements to Cyber Test Measurements

The SSE team and system developer perform requirements decomposition and flow-down, which forms the basis of cyber design information used to derive test metrics for a system's cybersecurity and cyber resilience characteristics; see Figure B-2.

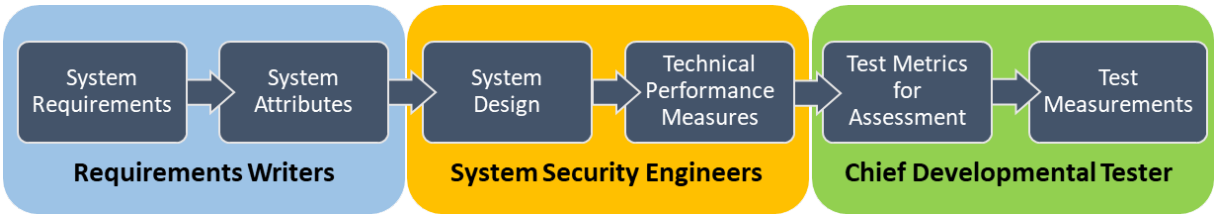


Figure B-2. High-Level Notional Overview of the Cyber Test Metric Derivation Process

B.2.1 Cyber Requirements and Cyber System Attributes

System requirements describe the system's intended performance. The requirements document often defines high-level descriptors (big "R" requirements) of the intended capabilities that the system should provide or functions that it should perform.

Ideally, requirements writers generate a tailored set of system cybersecurity and cyber resilience functional and performance requirements. Systems engineers use these requirements to produce a system design and the technical system requirement specification documentation, which further specifies the required level of cybersecurity and cyber resilience. System security engineers and the CyWG must ensure that cyber is part of the operational risk trade space for other functional requirements by articulating how the tailoring of system configuration settings, functionality, and other system design characteristics (e.g., AT, safety, redundancy) support or compete with system cyber resilience requirements. The CyWG should ensure that the contract requires the delivery of a requirements verification and traceability matrix, and the CyWG should use it to track system developer cyber tests to verify the requirements.

Latency Measurement Requirement in Concurrent T&E Example

The system may have a requirement for execution authorization decisions to be less than 31 milliseconds. (Expressed as explicit logic: if: application requests kernel resources, and if: application authorization is false, then: deny resources and log request, elapsed time less than 31 milliseconds.)

Test teams may determine that the SUT meets this criterion if, during simulated operations, the test team measures an average of 27 milliseconds for a STAT-determined statistically significant number of attempts.

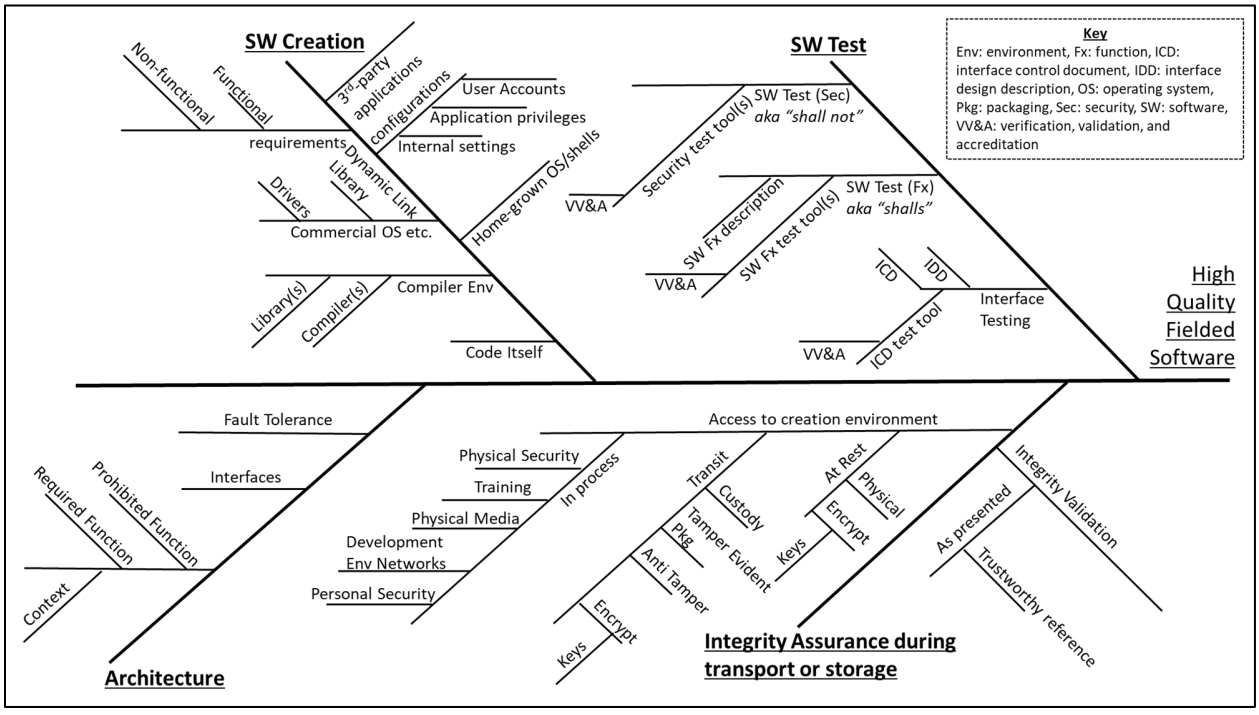
However, context matters when introducing cyberspace events in concurrent testing. For example, if introducing adversarial techniques during the simulated operations to cause cyberspace events to increase the decision to 15 seconds, two findings may be possible:

- **Finding A**: The system is not resilient if the system design is not resilient to the specific fault (for example, the latency is sufficient to cause the virtual private network (VPN) to break sync, and the entire VPN tunnel fails). In this case, there are two findings: (1) the system cannot meet the latency requirement of less than 31 milliseconds, and (2) the system is not resilient to the fault. Resolving either DR will ensure mission success.
- **Finding B**: The system is resilient if the system design requirements (e.g., resilience, redundancy, fault/tolerance properties) mitigate the increased latency, and mission execution is unaffected.

Exploitable design features are intentional functions that the procuring organization requires for the product. The test team could create an abuse case to potentially misuse these features and compromise the intended purpose of the operational mission system. Often, systems engineers do

not consider or address potentially adverse use cases during the requirements development process. Including the cyber test team representatives (e.g., penetration testers, red team testers) can optimize the process as these teams are the best available cyber threat emulators to represent the threat more accurately and bring exploitation insights to the process. Mitigating the exploitable design features may involve preventing access to them or altering the required design and operational usage to eliminate the need for them. The CyWG should identify the requirements, both at the individual technical level and at an architectural level, intended to mitigate the exploitation of design features by both accidents and adversaries. Additionally, the CyWG should understand what requirements are in place to reduce/prevent exploitable flaws (both in the choice of standards and in software assurance measures). The CyWG can assist the developers in balancing safety, security, and SSE requirements as a comprehensive set.

Figure B-3 demonstrates an Ishikawa format. Also known as a fishbone diagram or cause-and-effect diagram, the Ishikawa is a tool for systematically identifying potential root causes of problems. To reduce software risk, each branch should be correct. The CyWG may be able to use a similar depiction to advise on refining cyber performance requirements, scope cyber DT&E, and establish metrics.



Source: MITRE

Figure B-3. Ishikawa Diagram for Reducing Software Risk

"High quality fielded software" as depicted as the example fish bone head in Figure B-3 is not just about bug-free code. It means software that reliably maintains its security posture while meeting its functional and performance requirements in a real-world operational environment.

The CyWG should analyze what "high quality" means specifically from a cyber performance perspective. The diagram may help translate the abstract goal of "high quality" into specific, measurable cyber performance requirements. For example:

- *The Intrusion Detection System must maintain a threat detection rate of >95 percent with a false positive rate of <1 percent.*
- *Vulnerability patches must be deployed to production systems within 72 hours of release.*
- *The system must be able to withstand a distributed denial of service attack of X Gbps without significant performance degradation.*

B.2.2 Cyber System Design and Cyber Technical Performance Measures

During requirements analysis, the system developers' system security engineers define specifications for each contributing component and subcomponent to ensure the integrated system achieves the required overall performance. They develop a requirements verification traceability matrix to ensure lower-level decomposed requirements are traceable to the mission objectives. During the system development phase, supporting technology matures; developers create, integrate, and test prototypes; and the overall design evolves as engineers evaluate the initial assumptions. The objective during development is to use various measures and metrics, including TPMs and relevant leading indicators, to gauge technical progress against planned goals, objectives, and requirements. A subset of TPMs will be testable during a DT, forming the technical basis for deriving test metrics and measurements. For a sizable system, TPMs can number in the thousands. See the DoW Systems Engineering Guidebook for more details.

B.2.2.1 Cyber Technical Performance Measure for Resilience

The CyWG should plan to assess system cybersecurity and cyber resilience through the collective analysis of a system's cyber performance derived TPMs. The CyWG activities throughout *Iterative Planning for Cyber DT&E* help the CyWG understand the mission impacts of findings during test events. *Iterative Planning for Cyber DT&E* can help pare down the tests and metrics necessary for verifying the requirements. An example of a cyber TPM could be as follows:

- Example: The percentage of system state alerts captured hourly onto backup systems, assessed with each new capability release.

TPMs for cyber resilience are unique to the specific system or component design, functions, interfaces, and the operational mission. The CyWG should recurringly examine cyber resilience and cyber resilience requirements and begin to analyze TPMs early, before finalizing detailed

designs. The CyWG should iterate the analysis during development to ensure that the design enables testing for key measurements (e.g., a diagnostic port for testing, test support systems for measuring).

B.2.3 Cyber Technical Performance Measures to Cyber Test Metrics

Leveraging the TPMs, requirements documentation, and CONOPS, the SE team is responsible for generating a list of critical subcomponent, component, and system features to help attain desired operational performance capabilities (in the mission context). From this list, the CyWG should create a list of critical technical parameters (CTPs) for cyber resilience, which are metrics assessing the progress of the system in achieving these critical operational performance capabilities. These CTPs should be either a subset from the TPM list or directly traceable to the TPMs. Good CTPs and test metrics should not be simple restatements of KPPs or key system attributes (KSAs), as these are high-level descriptors of the system, not technical parameters of system or component attributes. Just as with TPMs, CTPs are unique to a system's specific functions, operational missions, and intended operational/mission environments and therefore are not generalizable across the scope of systems that DoW acquires.

B.3 Refine and Improve Measures and Metrics

Throughout the development process, regular discovery through MBCRAs and system developer testing validates some assumptions and invalidates others, leading to evolution in the system design. Because metrics relate to system design, the CDT or T&E lead, the CyWG, and SE teams should work together at regular intervals to update the CTPs and other test metrics when threats and technology changes invoke a design change or configuration change. For example, an early MBCRA might discover potential weaknesses in the designed security mechanisms or another way to employ the existing design to avoid a specific threat vector. Alternatively, if test teams cannot collect the data needed to verify the metrics, the SE team may need to alter the design to make measurement possible. In addition, updates to the threat assessment by the intel support during system development will occur as new intelligence becomes available. Appendix D: discusses the processes for requesting updated threat intelligence throughout the system's life cycle.

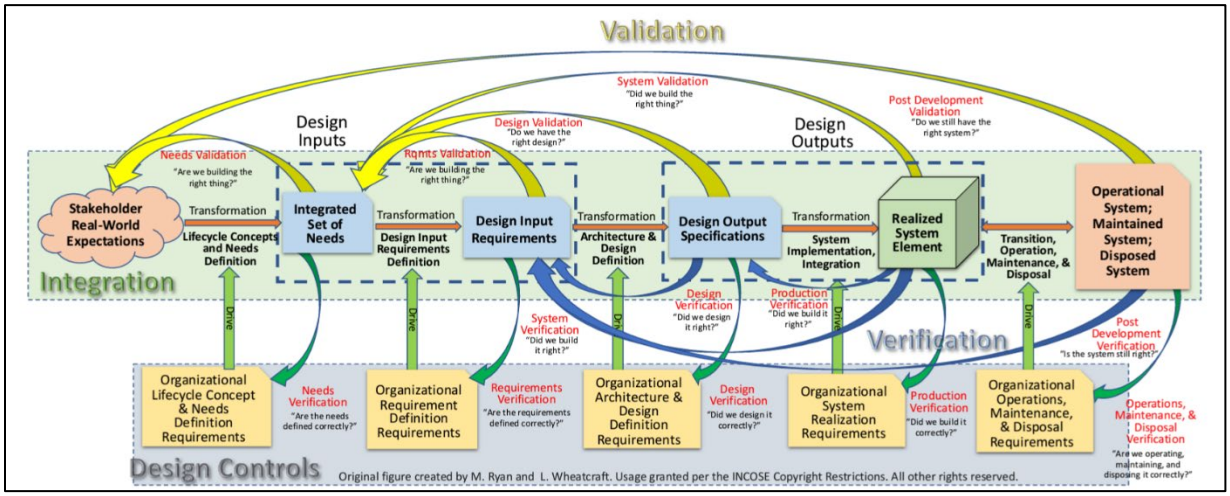
B.4 Metrics and Test Planning

This section covers the characteristics of good test metrics and briefly discusses some principles of test planning and reporting to ensure the collection and reporting of sufficient data to satisfy the evaluation of the CTPs.

B.4.1 Characteristics of Good Test Metrics

The CyWG is responsible for supporting the CDT or T&E lead in planning cyber tests that provide clear, relevant, and robust data (e.g., objective quality evidence) to inform decision makers. A well-chosen set of test metrics is a powerful tool in this process. The INCOSE Guide to Writing Requirements is a useful reference, as are the *Iterative Planning for Cyber DT&E* activities and tasks.

Figure B-4 from the INCOSE guide depicts using V&V throughout the life cycle. The depiction is generic and independent of a DoW acquisition, acquisition pathway, S&T project, or another distinct development effort and illustrates the continuum of testing feedback to system design, which enables data-informed decisions about the system and the overarching capability.



Source: International Council on Systems Engineering

Figure B-4. Verification and Validation Occurs Throughout the Life Cycle

Table B-2 describes five criteria to guide the evaluation of test metrics for incorporation into T&E plans. The DoD Software DT&E in DevSecOps Guidebook (https://www.cto.mil/dtea/software/) also provides guidance on uniquely software-related concerns.

Table B-2. Characteristics of Good Test Metrics

Relevant to the Mission	
Definition: A metric relevant to the mission enables assessing that a feature or attribute is easily and intuitively traceable to the system's mission or a mission-essential function.	Justification: The more clearly a metric connects to a mission-essential function through the mission decomposition to key cyber terrain (see Section 3), the more easily stakeholders can incorporate the metrics assessment into their decision-making process. Baselined using a functional requirement, measuring the operational resilience component requires emulating contested cyberspace.

<table>
<tr><td colspan="2">Example:
• Bad Metric: The frequency of automated configuration audits during simulated peak mission use loads is less than one per hour.
• Good Metric: The time to reestablish the system configuration from backups after a cyber intrusion during mission operations is less than 60 minutes.</td></tr>
<tr><th colspan="2">Easily Measurable/Assessable</th></tr>
<tr><td>Definition: A metric is easily measurable if it is directly measurable or if a simple model supports fusing data from several measurements to support the metric assessment. For qualitative metrics, the metric should be clear and definitive, not purely subjective.</td><td>Justification: Some of the most intuitive metrics are not readily measurable in a reliable way. Balance the other criteria with the ease of directly measuring attributes or observable characteristics to support the metric.</td></tr>
<tr><td colspan="2">Example:
• Bad Metric: The ease of access for outsider threat is low.
• Good Metric: Less than five logical access pathways exist to key data from external system interfaces.</td></tr>
<tr><th colspan="2">Robust to Varying Test Conditions</th></tr>
<tr><td>Definition: If a metric assessment is insensitive when unimportant environmental variables (e.g., test team skill, mission condition) change, then the metric is robust.</td><td>Justification: If insignificant changes to test conditions drastically change the metric results, then the derived information does not describe an intrinsic characteristic of the system, and the metric is not reliable.</td></tr>
<tr><td colspan="2">Example:
• Bad metric: The time to penetration by the red team (varies by the skill of the red team, mission conditions, etc.) is greater than 1 day.
• Good metric: The number of system accesses required to reach protected system data from all access points is greater than 12.</td></tr>
<tr><th colspan="2">Orthogonal (not redundant)</th></tr>
<tr><td>Definition: A metric is orthogonal if it produces information not derived by any other metric.</td><td>Justification: Because of limited time and resources, derive metrics to have as little overlap as possible to maximize information from a test.</td></tr>
<tr><td colspan="2">Example:
• Bad Metrics: (1) Less than 90% of passwords for all user accounts meet complexity requirements. (2) Less than 60% of user account passwords cracked in 6 hours using standard cracking tools.
• Good Metrics: (1) 100% of user account passwords meet complex requirements. (2) Demonstrated ability to identify and delete all orphaned accounts in 1 hour.</td></tr>
<tr><th colspan="2">Cover Data Needs</th></tr>
<tr><td>Definition: A set of test metrics covers the data needs producing enough information to inform knowledge points or decisions.</td><td>Justification: When defining the set of test metrics, the CyWG should ensure that the test metrics assess all critical parameters. Use scientific test and analysis techniques (STAT) to design tests covering the data needs.</td></tr>
</table>

No example given: Cover data needs is a characteristic of the entire set of metrics. Conduct analysis to ensure assessment of each cyber requirement by an appropriate set of metrics and that the test plans will holistically deliver adequate data to the data repository. A STAT expert on the CyWG facilitates achieving this characteristic.

B.4.2 Test Planning and Reporting Considerations

Although there are numerous factors that a test planner should consider, most are beyond the scope of this appendix. Poor test planning usually leads to tests producing poor or insufficient data. The following three aspects of often-overlooked test planning and reporting significantly affect the measurement of test metrics. DoW policy requires all three.

Data Collection. Test plans should require and allocate the resources necessary to collect both measurement data and data regarding the measurement collection procedures. Measurement collection information is specific to each type of measurement and may include the system configuration during the measurement and the assumptions used to create the system's simulated mission environment. Adequate planning to instrument and monitor the system during testing is necessary to capture these data. These kinds of data are critical in post-test analyses for understanding the uncertainty and robustness of metric assessments. Data collection should include information on how the test team collected test measures; how the test team applied assumptions and caveats during the analysis; and any quantifiable uncertainty in the measurements. Cyber test teams should consider ahead of time any protection required for collected test data, such as data at rest, in transit, or in combination with contextual/metadata. For cyber testing, the cyber analyst and cyber DT&E lead, as described in Appendix A:, are responsible for documenting this information throughout the cyber DT&E activities.

Statistical Rigor. Gathering quantitative metrics requires statistical rigor in the quantity and frequency of tests, where the measures are continuous variables. Including a statistician on the CyWG—responsible for reviewing test and reporting plans beforehand, assisting with a design of experiments approach, and reviewing a data analysis plan—is essential to inform test planning and ensure that the span of planned tests gather statistically relevant data to meet a specified confidence level. The current configuration, operating mode, environment, and users can significantly affect the security posture of a system. The CyWG should understand the amount of required testing necessary to ensure efficient and effective assessment of the system's cyber resilience and an appropriate representation of expected use conditions and configurations. Determining the amount of required testing involves understanding the risks associated with the operational mission and the ability to assess or not assess areas with actual testing. MBCRAs are useful in providing an understanding of the risks associated with gaps in testing scope.

Test Planning Process Rigor. Fundamental to the success of the test planning process and consequently the generation of defensible test metrics is the rigor of the overall test planning

process itself. Best practices are available for formally assessing T&E plans to ensure reliance on precise, consistent, and repeatable objective measures.

To produce defensible test results and effectively support decision makers, the CyWG should include experts in STAT (see Section 2.4). STAT enables the development of efficient, rigorous test strategies and is essential to achieving these goals.

Appendix C: Key System Artifacts for Cyber DT&E Analysis and Planning

This appendix provides key system artifacts for the CDT or T&E lead, CyWG, and cyber test team to analyze and use for cyber DT&E. Table C-1 lists and describes the most common artifacts for S&T and pre-acquisition projects and the AAF pathways. The table identifies a specific acquisition pathway for each artifact, as applicable. The absence of a pathway may indicate that the artifact applies to all non-acquisition and pre-acquisition pathways. Table C-2 lists potential sources of testable areas to inform the scope of testing during *Iterative Planning for Cyber DT&E*. The CyWG should research the appropriate documents.

Table C-1. Artifacts Supporting Test Planning Guidance

Artifacts <Relevant Pathway>	Content Description
Acquisition Strategy <Software and Middle Tier of Acquisition (MTA) pathways>	Includes high-level T&E, tailored test plans, the cybersecurity strategy, and proposed documentation tailoring.
Anti-Tamper (AT) Plan (appendix to the Program Protection Plan (PPP)) NOTE: AT Plans are not applicable to science and technology (S&T) and pre-acquisition projects.	Describes the systems engineering (SE) and systems security engineering (SSE) activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems, training devices, and maintenance support equipment. If the program management office is implementing AT, the PPP will document the critical program information (CPI) expected to employ AT and the specific AT countermeasures relevant to the threats and vulnerabilities to the CPI.
Architectural Operational Viewpoints (OVs) System Viewpoints (SVs) Data and Information Viewpoints (DIVs) or model-based systems engineering artifacts	These artifacts include: • OV-1: High-Level Operational Concept Graphic and OVs as needed • SV-1: Systems Interface Description • SV-2: Systems Resource Flow Description • SV-6: Systems Resource Flow Matrix • DIV-1: Conceptual Data Model (addresses operational architecture high-level information concepts) • DIV-2: Logical Data Model • DIV-3: Physical Data Model
Authorization boundary diagrams including systems and dataflows	Describes the system parameters and boundaries for the security controls assessment.
Capability Implementation Plan <Defense Business System (DBS) pathway>	Contains the capability description, business system acquisition approach, test and technical assessment strategies, integrated master schedule, and support strategy. NOTE: Artifact may not be a single document but a series of documents.

Artifacts <Relevant Pathway>	Content Description
• Capability requirements document: – Initial Capabilities Document (ICD) – Capability Development Document (CDD) – Capability Needs Statement <Software and MCA pathways> • System functional requirements <DBS pathway> • Urgent operational needs <Urgent Capability Acquisition (UCA) pathway> • Product roadmap <Software pathway> • Decision authority–signed Acquisition Decision Memorandum with a succinct requirements document <MTA pathway>	Provides cybersecurity and cyber resilience requirements. Includes the Cyber Survivability Risk Category assigned during the Cyber Survivability Endorsement Implementation Guide process or other means. The documents contain system performance requirements and specifications including: • Measures of effectiveness (MOEs) • Measures of performance (MOPs) • Critical operational issues (COIs) • Key performance parameters (KPPs) • Key system attributes (KSAs)
• Concept of operations (CONOPS) • Concept of employment (CONEMP) • User manuals	Describes the system's employment in operations and how people will use, maintain, and interact with the system. These documents should describe how users, defenders, and maintainers monitor the system, mitigate cyber threat activity, and restore the system to its baseline state following an attack.
Contract or Request for Proposal (RFP) Sections C, L, M and Contract Data Requirements Lists	Contains cyber DT&E requirements for system developers. *Iterative Planning for Cyber DT&E* activities and tasks should inform the RFP with cyber DT&E requirements before releasing the RFP to industry. For more information, refer to Appendix I:.
Cybersecurity Maturity Model Certification (CMMC) Level 1 Assessment	CMMC Level 1 requires contractors that host Federal Contract Information on their systems to complete a Basic Assessment on the security requirements that correspond to the 15 basic safeguarding requirements specified in 48 Contract Federal Regulations 52.204-21, commonly referred to as the Federal Acquisition Regulations Clause, and upload the resulting score to the Supplier Performance Risk System. The Department's policies for CMMC implementation require Program Manager's and requiring activities to identify a CMMC level (1, 2, or 3) based on the type of information that will be processed, stored, or transmitted on contractor owned information systems. https://dodcio.defense.gov/ Portals/0/Documents/ CMMC/ModelOverview.pdf
Cybersecurity Service Provider (CSSP) support agreement and/or Information Support Plan	Documents the CSSP and defensive cyberspace operations organization and processes that will protect the system once it is fielded.

Artifacts <Relevant Pathway>	Content Description
Cybersecurity Strategy (CSS) (DoW or Component Chief Information Officer–approved document; appendix to the PPP or the Acquisition Strategy when the system development does not require a PPP)	Consolidates elements of various initiatives and activities relating to cybersecurity planning, implementation, and risk; outlines the implementation status of projected cyber activities, including defensive cyberspace operations plans, across all stages of a system's life cycle; and is required for all AAF pathways. Acquisition program offices and the system owners should actively review, update, employ, and maintain the CSS for the life of the system in accordance with DoDI 8580.1.
Hardware Assurance Plan (may be in the PPP or an appendix to the PPP)	Documents the plans for implementing technical mitigations for mission-critical functions and critical components.
Intellectual Property Strategy <Software pathway>	Identifies open-source and third-party components expected to be included in the development and test of the software.
Information Support Plan (ISP)	Supports interoperability tests and certification. identifies and documents information needs, infrastructure support, and information technology and national security systems interface requirements and dependencies focusing on net-centric, interoperability, supportability, and sufficiency concerns.
Interface Description Document <all>	Most systems interface with other systems or with legacy modules of the existing system. These system interfaces should have a trust determination levied on them within the system design, and test teams should plan to incorporate the information flow handling as part of their T&E.
Joint Common System Function List	Provides a common lexicon of system functions supporting development of the DoW Information Enterprise Architecture and solution architectures.
Joint Mission Essential Task List for joint missions or Service-specific Mission Essential Task List	Identifies those tasks most essential to assigned or priority missions.
• Life Cycle Sustainment Plan (LCSP) • Sustainment Plan <UCA pathway> • Life Cycle Product Support Strategy <Software pathway> • Product Support Strategy <MCA pathway>	The LCSP is the primary artifact governing the system's support and sustainment planning. Discusses the product support plans in the system's life cycle, including supporting people, processes, and technology. The Product Support Strategy documents system support packages.
Mission Based Cyber Risk Assessment	Identifies potential vulnerabilities and weaknesses in a system; assesses the associated risk to a mission; and prioritizes actions to test, mitigate, reengineer, analyze, or accept those risks. Includes assessments of potential attacks and

Artifacts <Relevant Pathway>	Content Description
	investigation of the attack paths for cyber aggressors.
Previous test results	Includes government, contracted developer, or other test results and security assessments performed on the system.
Product roadmap <Software pathway>	Provides a high-level visual summary mapping out the vision and direction of product offerings over time; describes the goals and features of each software iteration and increment. The CyWG should continually review and revise the product roadmap.
Product backlog <Software pathway>	Provides a list of updates, cyber issues, and features (also known as user stories) that developers prioritize every time a new iteration begins.
Program Protection Implementation Plan (PPIP) <not required for Software, MTA, UCA, DBS pathways>	Is a system developer-provided document describing how the system developer will implement the program protection requirements outlined in the PPP for safeguarding critical components, protecting critical program information, implementing ICT supply chain risk management (SCRM), and ensuring software assurance.
Program Protection Plan (PPP) <not required for MTA, UCA, DBS pathways>	Details the acquisition program's SSE activities including cyber resilient engineering; specifies threats, vulnerabilities, and countermeasures (including ICT SCRM) to mitigate risks to the program's technology, components, and information based on criticality analyses software and hardware assurance testing requirements including the development environment and processes, mission-essential functions, dependencies, and ICT supply chain illumination.
Security Classification Guide (SCG) (usually an appendix to the PPP)	Discusses the classification requirements for cyber vulnerabilities and aggregation. 
System Security Plan (SSP)	Provides an overview of the cybersecurity capability and the technical requirements for the system and describes the planned security controls to meet those requirements. 
Security Assessment Plan (SAP)	Documents the frequency of assessments and the type of assessment method; outlines the processes to assess controls; the SAP should synchronize with the TEMP or T&E strategy. 

Artifacts <Relevant Pathway>	Content Description
Software Assurance Plan (may be in the PPP or an appendix to the PPP)	Documents the plans for implementing technical mitigations for software-implemented mission-critical functions and critical software components.
System developer detailed system specifications, system design documents, developer (system developer or government) design documentation	Provides requirements traceability from system requirements to system design; evidence (data, metadata, reports) from developer (system developer or government) planning, design implementation, and testing activities for the system under development; system designs, wiring diagrams, and logical and physical network architecture diagrams; and a list of hardware and software (COTS/GOTS) components and versions.
Systems Engineering Plan (SEP) or Systems Engineering Management Plan <not required for Software, MTA, UCA, DBS pathways>	Outlines the systems engineering approach, technical performance measures, and critical technical parameters.
System Interface Control Document	Is a document for each authorized system interface detailing the technical components, information exchanges, and points of contacts.
• System Performance Specification (SPS) • System Requirements Document (SRD) • Software Requirements Specification (SRS)	Defines the system-level requirements, constraints, interfaces (functional, performance, and design), and environmental considerations, derived from the CDD and CONOPS, and describes the qualification conditions and procedures for their testing and acceptance.
TEMP or T&E Strategy	Outlines the T&E approach (who, what, where, when, and how at a high level), including prototypes and operations demonstrations.
Transition Plan <MTA pathway>	Describes the approach to prototyping technology and whether or how the prototype capability transitions to a program of record (POR).
• Validated Online Lifecycle Threat (VOLT) Report, cyber threat modules • Defense Intelligence Threat Library • Service/Component cyber threat intelligence (CTI) • Publicly available CTI	Provides system-relevant cyber threats, including technological threats and assumed threats, and cyber critical intelligence parameters, if any. For more information, refer to DoDI 5000.86 and Appendix D:.
Waveform Analysis Application (WAA) (see DoDI 4630.09)	Establishes requirements for new or modified waveforms. The WAA may be for a specific POR or non-developmental item waveform. Both types of analysis require the WAA process.

As previously mentioned, Table C-2 lists potential sources of testable areas to inform test scope during *Iterative Planning for Cyber DT&E*. The CyWG should research the appropriate documents.

Table C-2. Potential Sources to Inform Iterative Planning for Cyber DT&E

Source	Testable Areas	Purpose	Location
AT requirements	Countermeasures employed to protect CPI from unauthorized access, reverse engineering, modification, or destruction. See Appendix L.	The countermeasures are meant to prevent adversaries from exploiting vulnerabilities to compromise functionality, steal intellectual property, or introduce malicious capabilities in software and hardware. AT controls can have cyber implications.	• PPP/AT Plan appendix • PPIP • RFP or contract • Acquisition Strategy • Capability Implementation Plan (DBS pathway)
COIs (as determined by operational test representatives)	High-impact concerns which may or may not significantly hinder a system's ability to perform its essential functions and meet mission needs in a real-world operational environment. Use to plan integrated cyber testing.	Identifies the questions for a determination of operational effectiveness, suitability, and survivability.	• TEMP • T&E strategy • Test strategy • Test plans • IDSK
CSSP support agreement or DCO plan	Informs testing DCO protections as described in the CSSP support agreement, CSS, or DCO plan.	Establishes a framework for proactive and reactive cybersecurity support, including the people, processes, and technologies required to enable a provider or an organic protection capability.	• PPP/CSS appendix • PPIP • LCSP • Acquisition Strategy • Capability Implementation Plan (DBS pathway)
CEEC	As required to support cyber DT&E of CEEC acquisitions. See DoDI O-3600.03.	CEEC may or may not require cyber T&E.	• Documentation for the CEEC acquisition • DoD CEEC T&E Standards Guidebook • DoDI O-3600.03
Cyber-EW operations	Cyber-EW implications on mission operations. Afford consideration to any forms of electromagnetic	Over-the-air electromagnetic transmission is one mechanism that adversaries could employ to degrade weapon system capabilities.	• System documentation • Visual inspection • Waveform analysis application (see DoDI 4630.09 for more information)

Source	Testable Areas	Purpose	Location
	radiation. See Appendix L.	Identifying apertures and communications standards informs test planning.	
CSAs	Measure the cyber performance specified in the CSAs or in the requirements for cyber resilience. The developer should decompose and allocate requirements into the detailed system design specifications. See Appendix B:.	CSAs or cyber resilience requirements provide specific performance requirements and should be measurable and testable for evaluation via T&E. If CSAs are absent from a system's requirements, then refer to systems engineers for resolution.	• Capability requirements document: ICD, CDD, SPS, SRD, SRS, CNS (Software pathway) • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • Acquisition Strategy • Capability Implementation Plan (DBS pathway)
Cyber threat intelligence	Details the capabilities and intents of cyber threats. Test teams need this information to emulate a validated cyber threat during adversarial testing. Test planning should assume that the threat possesses all unclassified information about the system and its operational environment. *Iterative Planning for Cyber DT&E* activities and tasks enable collection of documentation and the identification of systems engineers and personnel with specific expertise and comparable levels of access and resources.	Intelligence information on adversary cyber objectives, targets, and capabilities, including attack techniques, tactics, and procedures, should inform test planning and should shape cyber DT&E of the attack surface, countermeasures, and defensive techniques.	• VOLT Report, cyber threat modules, Defense Intelligence Threat Library • Service-specific Threat Assessment Report • Other cyber intelligence documents, as appropriate and available • See Appendix D: for more information
Financial system requirements	Cyber economic evaluators assess the key operational capabilities and business processes.	A cyber threat may intend to influence the flow of financial resources.	• Capability requirements document: ICD, CDD, SPS, SRD, SRS, CNS (Software pathway) • System functional requirements (DBS pathway)

Source	Testable Areas	Purpose	Location
			• Capability Implementation Plan (DBS pathway) • Transition Plan (MTA pathway) • Technology readiness reviews • RFP or contract
Hardware and software assurance plans	Describe the security of hardware and software developmental items, including ICT SCRM activities.	The PPP or the appendices define threats, vulnerabilities, and countermeasures. The CyWG should understand the hardware and software assurance testing and analyze the plans and data to inform cyber T&E scope.	• PPP, LCSP, PPIP • Hardware and software assurance plans • Intellectual Property Strategy, product roadmap, product backlog (Software pathway) • Anti-Tamper Plan • System Design and Interface Control Documents • Developer documentation • TEMP, T&E strategy, previous test results • DoW RMF Security Plan and SAP • Acquisition Strategy • Capability Implementation Plan (DBS pathway)
Interoperability	interoperability is a component of security (e.g., cyber DT&E may help determine whether devices exchanging data through external interfaces enforce the principle of least privilege).	Programs test and evaluate systems to ensure that the systems achieve information technology interoperability requirements, including when they are operating in contested cyberspace.	• CDD • Capability Implementation Plan • DoDAF products: OVs, SVs, Data and Information Viewpoints • Information Support Plan • SEP • TEMP or T&E strategy • Interface Control Documents
MBCRAs	Identify the current cyber risk posture for the system; test high-risk components and interfacing systems that may contribute to mission risk of failure.	Provide opportunities to identify potential design problems and inform the T&E planning to encompass high-risk components and data exchanges.	• MBCRA Report (See Appendix G:)

Source	Testable Areas	Purpose	Location
MOEs	Capture the ability of a unit equipped with the system to complete mission objectives and achieve the desired results.	Assess with and without cyber aggression, inform the assessment of the system and resolution of issues for the event.	• Capability requirements documents: ICD, CDD, SPS, SRD, SRS, CNS (Software pathway) • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • Acquisition Strategy • Capability Implementation Plan (DBS pathway) • TEMP or T&E strategy • Test strategy • Test plans • IDSK
MOPs	Capture a system's performance typically using a characteristic of the system or its operation (e.g., speed, payload, range).	Assess with and without cyber aggression, inform the assessment of the system and resolution of the issues for the event.	• Capability requirements document: ICD, CDD, SPS, SRD, SRS, CNS (Software pathway), OV-5bs • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • Acquisition Strategy • Capability Implementation Plan (DBS pathway) • TEMP or T&E strategy • Test strategy • Test plans • IDSK
Measures of suitability	Measure the ability to support an item in its intended operational environment. These measures typically relate to readiness or operational availability and, therefore reliability, maintainability, and the item's support structure.	Assess with and without cyber aggression, inform the assessment of the system and resolution of the issues for the event.	• TEMP or T&E strategy • Test strategy • Test plans • Operational Evaluation Framework

Source	Testable Areas	Purpose	Location
Mission-critical or mission-essential functions (and a description of the relationship to one another)	Enumeration of functional properties (and conditions) required for mission success.	Required to bound the space of negative functionality to only those functional failures that can plausibly deny the mission; also, to balance protection and safety requirements with mission accomplishment.	• MBCRA results aligned to ICD, CDD, CONOPS, CONEMP
Mission operation in contested cyberspace, composite, and other threat environments	Describe cyber and operational concepts.	Derive cyber and operational resilience requirements from mission descriptions to ensure required mission operation.	• Capability requirements document: TRD, CDD, SPS, SRD, SRS, CNS (Software pathway) • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • Acquisition Strategy • Capability Implementation Plan (DBS pathway) • CONOPS and CONEMP • OVs
Mission operational parameters	Define the complete end-to-end mission(s) in terms of characteristics such as mission purpose, schedule, execution, and resources.	Decomposition of the end-to-end mission enables inclusion of cyber effects with functional T&E and identifies sources of inherent and inherited risk.	• Mission CONOPS, OV-1, and other mission documents • SPS, SRD, SRS • Mission Essential Task Lists • Common System Function Lists • Acquisition Strategy • Capability Implementation Plan (DBS pathway)
Other sources	Cyber Survivability Risk Categorization and the DoW RMF categorization both imply acceptable cyber risk for the system's confidentiality, integrity, and availability protections.	The T&E strategy should outline testing with an appropriate scope and depth to confirm that the system can maintain the data confidentiality, integrity, and availability required to support completion of the unit's mission.	• ICD, CDD, CNS (Software pathway) • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • DoW RMF Security Plan 

Source	Testable Areas	Purpose	Location
			• CSS • Acquisition Strategy • Capability Implementation Plan (DBS pathway)
Physical information architectures and dataflows	Determine the electrical connectivity and intended flow of information between system components and between the system and its operational environment.	Informs test infrastructure planning; the data exchanges and interfaces are part of the attack volume and may require testing. This information is part of the basis for a cyber test design.	• LCSP • Architecture OVs and SVs or MBSE artifacts • SCG • Developer documentation
Safety-critical functions (and a description of safety cases if built)	Describes the system functions required to achieve acceptable safety parameters.	Informs cyber test boundaries to avoid unsafe system performance. Allows cyber T&E to examine the safety impact of cyber cases.	• MIL-STD-882 analysis products • System safety analysis
Security controls	System developers test technical controls implemented in the system, and the government verifies that the controls do not support or enable threat-exploitable vectors.	Use security controls to achieve system protection goals; ensure selection of the controls listed in Appendix I:. Align technical security controls to the prioritized subcomponents, components, and subsystems.	• DoW RMF Security Plan or other DoW RMF documentation • DoW RMF authorization boundary diagrams including systems and dataflows • Developer documentation • RFP or contract
Security controls assessment	Ensures full implementation of the controls before planned security control testing.	Details the schedule and methodology for assessing security controls implementation.	• DoW RMF SAP • TEMP • T&E strategy • Previous test results
Security requirements and engineering specifications	Systems engineers decompose security requirements into the engineering specifications and designs that test teams examine.	Critical technical specifications and technical performance measures inform the cyber DT&E of components and subsystems.	• SEP, TRD, SPS, SRD, SRS • SCG • Developer documentation • Contract or RFP • Product roadmap, product backlog (Software pathway) • Acquisition Strategy • Capability Implementation Plan (DBS pathway)

Source	Testable Areas	Purpose	Location
Specialized components	Review the system for specialized data exchanges, such as cross-domain solutions and non–Internet protocol information exchanges. See the CUI Appendix L.	Informs test planning because specialized components may be mission critical and require long-lead test tools or teams.	• LCSP • Architecture OVs and SVs or MBSE artifacts • SCG • Developer documentation
Software assurance testing	Plan software testing based on the PPP definition of software developmental items including the development environment and processes. See the DoD Software DT&E in DevSecOps Guidebook.	The PPP describes software developmental items and the requirements for testing them; the DoD Software DT&E in DevSecOps Guidebook discusses considerations for planning and performing software assurance testing.	• PPP, LCSP • PPIP • System Design and Interface Control Documents • Developer documentation • TEMP • T&E strategy • Previous test results • Acquisition Strategy • Capability Implementation Plan (DBS pathway) • Intellectual Property Strategy • Product roadmap • Product backlog (Software pathway)
Supply chain protection	Review the ICT supply chain risk documented in the PPP, Acquisition Strategy, and Capability Implementation Plan (DBS pathway) to plan T&E for critical functions and components. See Appendix F:.	Understand the approach for managing ICT supply chain risks that may influence system design, development, or operations.	• PPP/ICT SCRM section • PPIP • LCSP • Developer documentation • Bill of materials • Acquisition Strategy • Capability requirements document: TRD, CDD, SPS, SRD, SRS, CNS (Software pathway) • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • Capability Implementation Plan (DBS pathway) • Contract or RFP

Source	Testable Areas	Purpose	Location
System-critical components and information	Prioritize testing of implemented countermeasures to protect CPI, mission-critical functions, and critical components; conduct concurrent cyber and non-cyber T&E (see Section 1.7).	Cross-reference with hardware and software assurance and AT; inform functional T&E approaches including cyber effects.	• PPP/criticality analysis appendix • PPIP • DoW RMF/ criticality analysis control (RA-9)
System data availability requirements	Inform adversarial testing of system data availability and recovery timeframes; conduct concurrent cyber and non-cyber T&E (see Section 1.7).	Examine the availability of the system data needed to support mission operations.	• MOEs, MOPs, COIs, KPPs, KSAs • MBCRA • CONOPS • CONEMP
System data confidentiality requirements	Inform the adversarial testing of system data confidentiality needs; conduct concurrent cyber and non-cyber T&E (see Section 1.7).	Inform the adversarial testing of system data integrity needs.	• MOEs, MOPs, COIs, KPPs, KSAs • MBCRA • CONOPS • CONEMP
System data integrity requirements	Inform the adversarial testing of system data integrity needs; conduct concurrent cyber and non-cyber T&E (see Section 1.7).	Examine the integrity of data needed to support mission operations.	• MOEs, MOPs, COIs, KPPs, KSAs • MBCRA • CONOPS • CONEMP
System key performance parameters (KPPs) and key system attributes (KSA)s	System capabilities or attributes that the system should meet to accomplish the operational mission, even in the presence of contested cyberspace threats.	Systems engineers derive cyber controls and countermeasures from an analysis of each KPP and KSA. Cyber DT&E should assess the impact of cyber effects on these performance thresholds.	• Capability requirements document: Information Systems ICD, Software ICD, CDD, CNS (Software pathway) • System functional requirements (DBS pathway) • UONs (UCA pathway) • Product roadmap (Software pathway) • Transition Plan (MTA pathway) • TEMP, T&E strategy, previous test results • Acquisition Strategy • Capability Implementation Plan (DBS pathway)

Source	Testable Areas	Purpose	Location
System recovery timeframe	Determine the maximum amount of time that users can take to mitigate a cyber threat during an attack and still complete their mission(s); conduct concurrent cyber and non-cyber T&E (see Section 1.7).	Time to recover is a measure of whether a unit equipped with the system can "fight through" an attack.	• CONOPS • CONEMP • MOEs, MOPs, COIs, KPPs, KSAs • RFP or contract • For mature systems or recapitalization efforts, the system may include this information in training, operations, or maintenance manuals.
System restoration timeframe	Determine the maximum amount of time that users and maintainers can take to restore the system to its state before an attack ("baseline") and still support its next mission(s); conduct concurrent cyber and non-cyber T&E (see Section 1.7).	Time to restore is a measure of whether a cyber threat can overwhelm the logistics solutions of the unit.	• CONOPS • CONEMP • MOEs, MOPs, COIs, KPPs, KSAs • RFP or contract • For mature systems or recapitalization efforts, the system may include this information in training, operations, or maintenance manuals.

Acronyms used in this table. AT: anti-tamper, CDD: capability development document, CEEC: cyberspace effects and enabling capabilities, CNS: capability needs statement, COI: critical operational issue, CONEMP: concept of employment, CONOPS: concept of operations, CPI: critical program information, CSA: cyber survivability attribute, CSS: cybersecurity strategy, CSSP: cybersecurity service provider, DBS: defense business system, DCO: defensive cyberspace operations, DoDAF: DoD architecture framework, EW: electronic warfare, ICD: initial capabilities document, ICT: information and communication technology, IDSK: integrated decision support key, KPP: key performance parameter, KSA: key system attribute, LCSP: life cycle sustainment plan, MBCRA: mission based cyber risk assessment, MBSE: model-based systems engineering, MIL-STD: Military Standard, MOE: measure of effectiveness, MOP: measure of performance, MTA: middle tier of acquisition, OV: operational viewpoint, PPIP: Program Protection Implementation Plan, PPP: Program Protection Plan, RFP: request for proposal, RMF: risk management framework, SAP: Security Assessment Plan, SCG: Security Classification Guide, SCRM: supply chain risk management, SEP: System Engineering Plan, SPS: System Performance Specification, SRD: System Requirements Document, SRS: System Requirement Specification, SV: system viewpoint, TEMP: Test and Evaluation Master Plan, TRD: Technical Requirements Document, UCA: urgent capability acquisition, UON: urgent operational need, VOLT: Validated Online Lifecycle Threat

Appendix D: Cyber Threat Assessment for Cyber DT&E

D.1 Background

Cyber threat assessments combine the understanding of known vulnerabilities within internal and external systems, architectures, and interfaces with real-world attack data and intelligence about threat actor TTPs and their strategic and tactical/system-level objectives. Acquisition programs use intelligence and counterintelligence validated threat reports to guide risk-based SE and trade-off decisions. The test community uses these same reports for test planning and execution. Cyber threat reporting enhances an acquisition program's data repository when the reporting is integrated into cyber DT&E activities. Threat reporting support should start during *Iterative Planning for Cyber DT&E* activities and tasks. Threat reporting significantly contributes to the *Planning*, *Preparing*, *Executing*, and *Evaluating* activities, and test teams should use threat reporting to contextualize test results during *Reporting Cyber DT&E Results*. The CyWG should seek to obtain cyber threat assessments early and receive updates regularly during all stages of the system's life cycle to:

- Enable proactively addressing adversary current and future threat capabilities and TTPs.
- Inform SE and system developer design decisions as cyber threats evolve.
- Verify cybersecurity and cyber resilience requirements.
- Characterize the attack surface including identifying susceptibilities, exposures, and exploitable vulnerabilities.
- Plan and conduct MBCRAs and comprehensive test events based on validated adversary capabilities and assessed intent.

Program manager organizations and the cyber DT&E community should plan for and reach out as early as possible to the DoW IC (which includes Service intelligence organizations) to obtain support for intelligence and counterintelligence cyber threat assessments. Effective and efficient utilization of the DoW IC should focus on:

- Initiating early contact with the appropriate Service intelligence organization(s) to request support.
- Developing intelligence needs to address RFIs generated during cyber DT&E events.
- Providing the IC with clear requests, guidance, and timely feedback to refine intelligence products, influence intelligence analyst research TTPs, and develop intelligence production requests (PRs).
- Providing clear intelligence needs to DIA for ICT supply chain analysis.

- Requesting intelligence analysts to convert system-level, adversary cyber threat "capability and intention" assessments into risked-based "opportunity and means" characterizations of adversary cyber threats to system designs, capabilities, and operating environments.

This appendix describes how to employ the IC, use IC cyber threat analysis TTPs, obtain cyber threat assessments, and obtain IC support for cyber DT&E events.

D.2 Schedule

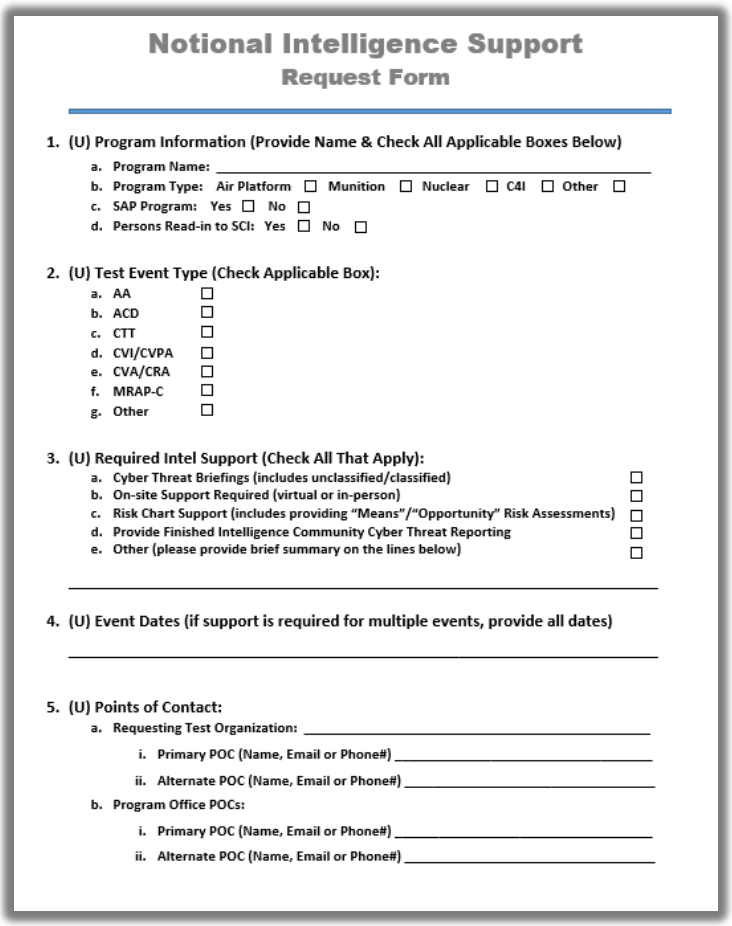
Acquisition programs should request intelligence threat assessments at program initiation with updates throughout the system's life cycle to support system development and major acquisition decisions. Non-acquisition or pre-acquisition projects should use this appendix and apply its guidance to request intelligence for their efforts. Although these intelligence products are useful, cyber DT&E requires focused, system-level threat assessments for test planning and execution. S&T projects and other pre-acquisition efforts should request IC support at the start of the project because of the typically shorter timelines associated with these efforts. Program manager organizations should request IC support during the initial scheduling stages of MBCRAs or other test events. Table D-1 highlights the actions for obtaining IC support for cyber DT&E.

Table D-1. Key Intelligence Support Actions

Action	Justification
Initiate Request for Intelligence Community (IC) Support as Early as Possible and Provide Timelines	Requesting organizations should request support from the IC (i.e., the assigned intelligence units and the supporting Intelligence Production Centers) as early as possible and provide reasonable suspense dates. The early request will help the responsible intelligence organization allocate the necessary time to provide detailed, system-specific cyber threat assessment support (i.e., conduct thorough research and analysis, generate necessary production requests, and construct briefings and other products).
Request Cyber Threat Support from Assigned Intelligence Organization	Requesting organizations should submit intelligence support requests to the organization assigned to the program. These organizations likely have intelligence analysts possessing system-level knowledge and some cyber-threat intelligence expertise. This knowledge base is essential to provide adequate cyber threat support during cyber DT&E events.
Identify the Required Intelligence Support	Requesting organizations should specifically request the type of support and products required (cyber threat briefs, cyber threat reporting, etc.) for cyber DT&E events. This specificity helps allocate time and other resources to facilitate event requirements.
Highlight Classification Requirements	Program classification requirements directly influence the resources that the IC can use to support cyber DT&E

Action	Justification
	events. Program classification requirements impact intelligence research tactics, techniques, and procedures; cyber threat reporting usage; and intelligence briefings. NOTE: Special access programs present additional challenges to the IC. Identify special access program requirements as early as possible.

Figure D-1 depicts a notional intelligence support request form.



Notional Intelligence Support
Request Form

1. (U) Program Information (Provide Name & Check All Applicable Boxes Below)
   a. Program Name: _____
   b. Program Type: Air Platform ☐ Munition ☐ Nuclear ☐ C4I ☐ Other ☐
   c. SAP Program: Yes ☐ No ☐
   d. Persons Read-in to SCI: Yes ☐ No ☐

2. (U) Test Event Type (Check Applicable Box):
   a. AA ☐
   b. ACD ☐
   c. CTT ☐
   d. CVI/CVPA ☐
   e. CVA/CRA ☐
   f. MRAP-C ☐
   g. Other ☐

3. (U) Required Intel Support (Check All That Apply):
   a. Cyber Threat Briefings (includes unclassified/classified) ☐
   b. On-site Support Required (virtual or in-person) ☐
   c. Risk Chart Support (includes providing "Means"/"Opportunity" Risk Assessments) ☐
   d. Provide Finished Intelligence Community Cyber Threat Reporting ☐
   e. Other (please provide brief summary on the lines below) ☐

   _____

4. (U) Event Dates (if support is required for multiple events, provide all dates)

   _____

5. (U) Points of Contact:
   a. Requesting Test Organization: _____
      i. Primary POC (Name, Email or Phone#) _____
      ii. Alternate POC (Name, Email or Phone#) _____
   b. Program Office POCs:
      i. Primary POC (Name, Email or Phone#) _____
      ii. Alternate POC (Name, Email or Phone#) _____

Source: U.S. Air Force 48th Cyberspace Test Squadron

Figure D-1. Notional Intelligence Support Request Form

D.3 Inputs

To provide detailed system-level cyber threat analysis to the program manager and cyber DT&E community, the IC needs system and system development documents and may need to communicate with the system design engineers. The CyWG should facilitate access to both the data repository and the government and system developer's design engineers to resolve any questions that the assigned intelligence analysts may have while trying to analyze the system's

architecture, diagrams, designs, characteristics, capabilities, etc. Table D-2 outlines baseline document inputs for intelligence support to cyber DT&E for acquisition programs. Intelligence analysts should work with the CyWG to determine what documents are available.

Table D-2. Supporting Documentation Inputs

Document(s)	Justification
Any Architecture, DoDAF, System Diagrams, or Related System Analysis Reports	Provides intelligence analysts with in-depth, foundational understanding of system designs including system overviews, architectures, components, data connections, and ICT supply chain information. These documents help drive preliminary intelligence community (IC) cyber threat collection, analysis, and reporting strategies for MBCRAs and other cyber DT&E events.
Technology and Program Protection Plans	Helps focus cyber threat collection and analysis tactics, techniques, and procedures (TTPs) by highlighting critical program information and critical components.
Security Classification Guides	Informs the IC on how to properly classify and handle specific information during cyber threat analysis.
All Program-Specific Cyber Threat Reporting (e.g., VOLT)	Provides intelligence analysts with previously reported system-specific cyber threat intelligence as a baseline while conducting additional research into system-specific information and evolving adversary cyber threat capabilities and TTPs.
All Program-Specific Counterintelligence Reports (Integrated Threat Assessments)	Enhances cyber threat analysis with human intelligence reporting and ICT supply chain threat data.

D.4 Derived Intelligence Needs

The IC uses a five step intelligence process to provide intelligence products to customers:

1. Planning and Direction.
2. Collection.
3. Processing and Exploitation.
4. Analysis and Production.
5. Dissemination and Integration.

To start this process, the CDT or T&E lead submits RFIs to the assigned intelligence organization. Assigned intelligence analysts should work with the CyWG and the program manager's organization representatives to derive intelligence needs from the RFIs. These intelligence needs justify in-depth, system-specific cyber threat analysis from the assigned intelligence organization and reporting from the rest of the IC via the PR process. T&E leads should also consider leveraging the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF is composed of nearly two dozen Federal intelligence, military, and law

enforcement agencies, along with local law enforcement and international and private industry partners. The task force serves as the government's central hub for coordinating, integrating, and sharing information related to cyber threat investigations.

D.5 Production Requests

- The CyWG's intelligence liaison should use a PR to request intelligence products from the IC or to request intelligence support for cyber DT&E events; see

Table D-3 for the contents of a PR. The program manager's organization should work with the assigned intelligence unit to develop the PR. Once the PR form is completed, the assigned intelligence organization will submit the PR form to the respective Service Intelligence Production Center (IPC) via the Community On-Line Intelligence System for End Users and Managers (COLISEUM). The Service IPCs listed below validate PRs for their respective Service branch:

- National Air and Space Intelligence Center.
- National Ground Intelligence Center.
- Office of Naval Intelligence.
- Marine Corps Intelligence Activity.

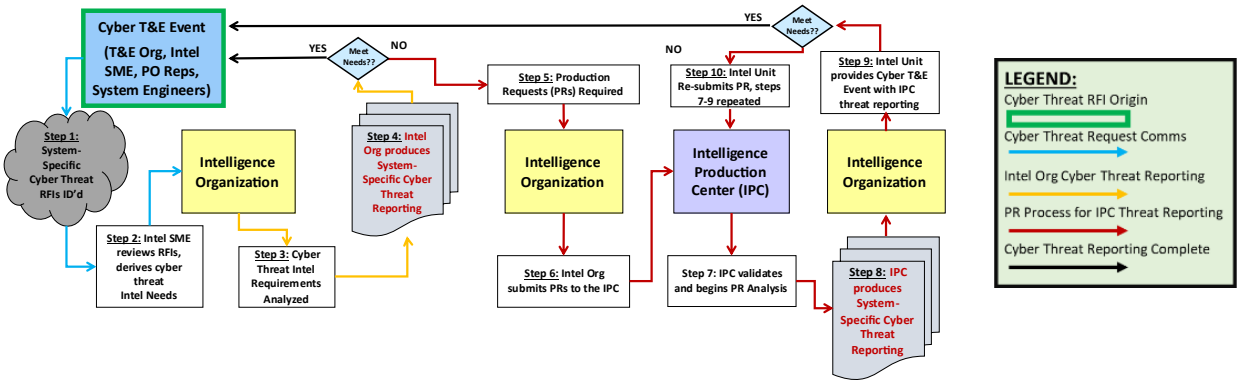
Table D-3. Typical Production Request Form Contents

Requirements	Justification
Intelligence Organization Name with Primary and Secondary Points of Contact (POCs)	Provides Intelligence Production Centers (IPCs) with intelligence organization POCs for analyst-to-analyst interactions to address IPC questions related to the production request (PR) submission.
Cyber Threat Intelligence Needs	Represents the information needed for system-specific cyber threat analysis. The CyWG and program manager's representatives work with the assigned intelligence unit to clearly define the required information. NOTE: This request can include one or multiple intelligence needs.
Target Adversaries	Provides the IPC with one or multiple adversaries on which to focus cyber threat analysis.
Suspense Timelines	Provides the IPC with a suspense date to complete the PR and deliver the requested finished intelligence product. This suspense timeline drives the intelligence process. NOTE: Shortened suspense times hamper the IPC's ability to generate more detailed system-specific finished intelligence reports.

Requirements	Justification
Cyber Threat Product(s) Classification Level	Provides the IPC with the classification level of the requested cyber threat product(s), for example if the finished cyber threat products should be delivered on the Secret Internet Protocol Router Network (SIPRNET). IPCs typically conduct analysis and disseminate finished intelligence products on the Joint Worldwide Intelligence Communications System.
Justification	Provides the rationale for the PR and influences the IPC's prioritization for answering the PR. Detail the justification and indicate the mission impact of the finished intelligence product. NOTE: The justification enables IPCs to prioritize PRs.
Cyber Threat Product(s) Format	Informs the IPC of the required finished intelligence reporting format (PowerPoint, PDF, Excel spreadsheet, etc.) to answer the PR.

Respective Service IPCs review, validate, and provide the requested finished CTI products for the PR. Source: U.S. Air Force 48th Cyberspace Test Squadron

Figure D-2 provides a flowchart of how derived cyber DT&E intelligence needs and PRs task the intelligence process to produce cyber threat reporting. System developers and DoW organizations may have unique processes to discover intel reporting that is relevant and releasable to them for their specific needs.



Source: U.S. Air Force 48th Cyberspace Test Squadron

Figure D-2. Intelligence Unit and IPC Cyber Threat Production Flowchart

D.6 ICT Supply Chain Threat Support

SCRM is a broad discipline. Traditional SCRM focuses on component quality, supplier stability, affordability, and the ability of suppliers to reliably deliver components to meet just-in-time production schedules. The ultimate risk in the traditional supply chain is that the systems integrator will not be able to procure and receive quality components needed to build the system for any array of reasons, many outside the integrator or supplier's control. Cybersecurity is the

practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks, damage, or unauthorized access.

C-SCRM manages the risk of protecting ICT, data, and information networks within and between suppliers. During MBCRAs, the MBCRA team usually identifies critical components and possibly other hardware, firmware, and software components of interest. The CyWG team prioritizes the components of interest for ICT supply chain threat analysis and follow-on testing. DIA is responsible for all-source threat analysis of ICT supply chain risk for acquisition programs. Within DIA, the SCRM Threat Analysis Center (TAC), if tasked, provides the acquisition community with specific threat characterizations of the suppliers for critical components or suppliers for other components of interest. Because of the protections afforded to U.S. persons and U.S. companies by intelligence oversight regulations, SCRM-TAC tasking will not use the IC PR process for threat support. Acquisition program managers should contact their respective DoW Component TSN focal point office to request ICT supply chain threat analysis.

In addition to the DIA SCRM-TAC analysis, local intelligence organizations can also provide the following ICT supply chain cyber threat support to T&E organizations. The support requires additional training and justification/approval from the appropriate authorities (to ensure no violation of intelligence oversight regulations).

- Deliver finished intelligence/counterintelligence cyber threat reporting to highlight adversary interests, capabilities, and activities enabling the possible exploitation of critical components.
- Gather unclassified open-source data on supplier activities.

Another resource for threat information is the Defense Counterintelligence and Security Agency (DCSA), which has established the capability to identify and track contested cyberspace activity directed at the defense industrial base (DIB).

D.7 Intelligence Metrics Used to Support Risk-Based Threat Characterizations

The IC includes adversary capability, intent (likelihood), and confidence level assessments as part of its cyber threat analysis reporting for a specific system. The IC characterizes adversary cyber threat capabilities by threat tiers. Table D-4 provides an overview of adversary cyber threat tiers used by the IC and DoW.

Table D-4. Intelligence Reporting Threat Tiers

Threat Tier	Description
Nascent	Little to no organized cyber capabilities, with no knowledge of a network's underlying systems or industry beyond publicly connected open-source information.
Limited	Able to identify and target for espionage or attack easily accessible unencrypted networks running common operating systems using publicly available tools.
Moderate	Able to use customized malware with better operational security practices to conduct wider-range intelligence collection operations; gain access to more isolated networks; and, in some cases, create short-duration effects against critical infrastructure networks.
Advanced	Have the capacity to conduct complex, long-term attack operations combining multiple intelligence sources to obtain access to high-value networks. Advanced actors can also develop the detailed technical and system knowledge of the target system necessary to deploy more damaging attacks.

The IC characterizes adversary intent into a specific set of likelihood ratings for IC finished threat reporting; see Table D-5 for IC terms and percentages.

Table D-5. Intelligence Reporting Likelihood Ratings

Rating	Description	Percentage
Almost No Chance	Remote	01%–05%
Very Unlikely	Highly Improbable	05%–20%
Unlikely	Improbable (Improbably)	20%–45%
Roughly Even Chance	Roughly Even Odds	45%–55%
Likely	Probable (Probably)	55%–80%
Very Likely	Highly Probable	80%–95%
Almost Certain(ly)	Near Certain	95%–99%

The IC ascribes high, moderate, or low IC confidence levels to each capability and likelihood cyber threat assessment. IC confidence levels express the strength of the assessment given the reasoning; methodologies; intelligence gaps and assumptions; and number, quality, and diversity of sources and the potential for deception. Table D-6 provides a brief description of each confidence level.

Table D-6. Intelligence Reporting IC Confidence Levels

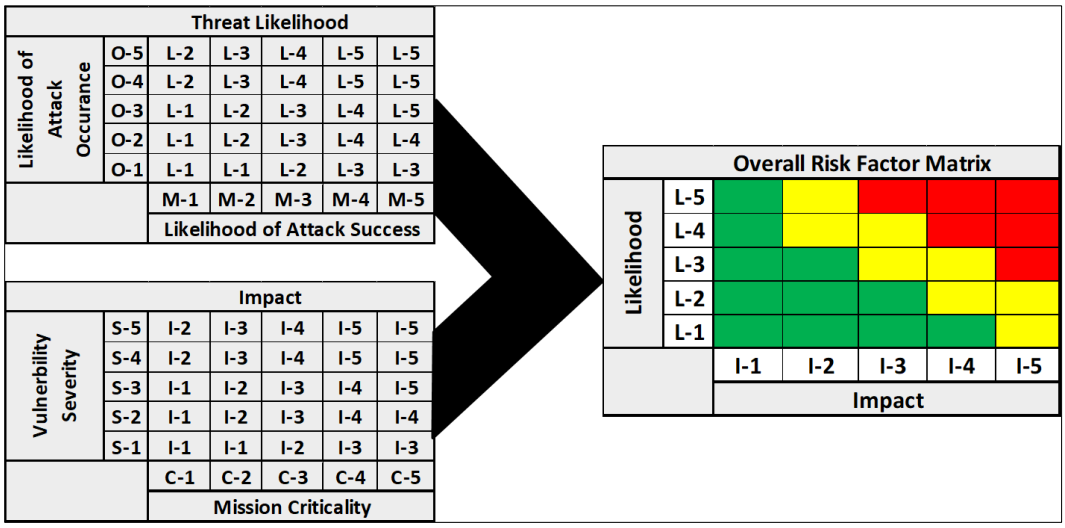
Level	Description
High	Generally indicates that sound reasoning and/or methodologies have been applied; no linchpin assumptions have been made; no critical gaps relevant to the issue are evident.
Moderate	Generally indicates that potentially critical assumptions are used to fill gaps; some inconsistencies exist, but the preponderance of evidence supports the judgment.
Low	Generally indicates that key assumptions have been used to fill critical gaps; significant inconsistencies or questions exist regarding the evidence; the information is fragmented or uncorroborated or is of questionable credibility and/or plausibility.

Program manager organizations should use these intelligence likelihood cyber threat assessment ratings to help identify and prioritize cyber risks for decisions and cyber testing. Intelligence analysts support this need by:

- Extracting adversary capability, intent (likelihood), and confidence level assessment data from finished high-level and system-specific IC cyber threat reports.
- Converting the capability, intent, and confidence intelligence assessment language into "means and opportunity" threat ratings.

For cyber DT&E events using risk-level determination matrices, the CyWG will need to submit requests to supporting intelligence organizations to provide threat likelihood scoring.Source: U.S. Air Force 48th Cyberspace Test Squadron

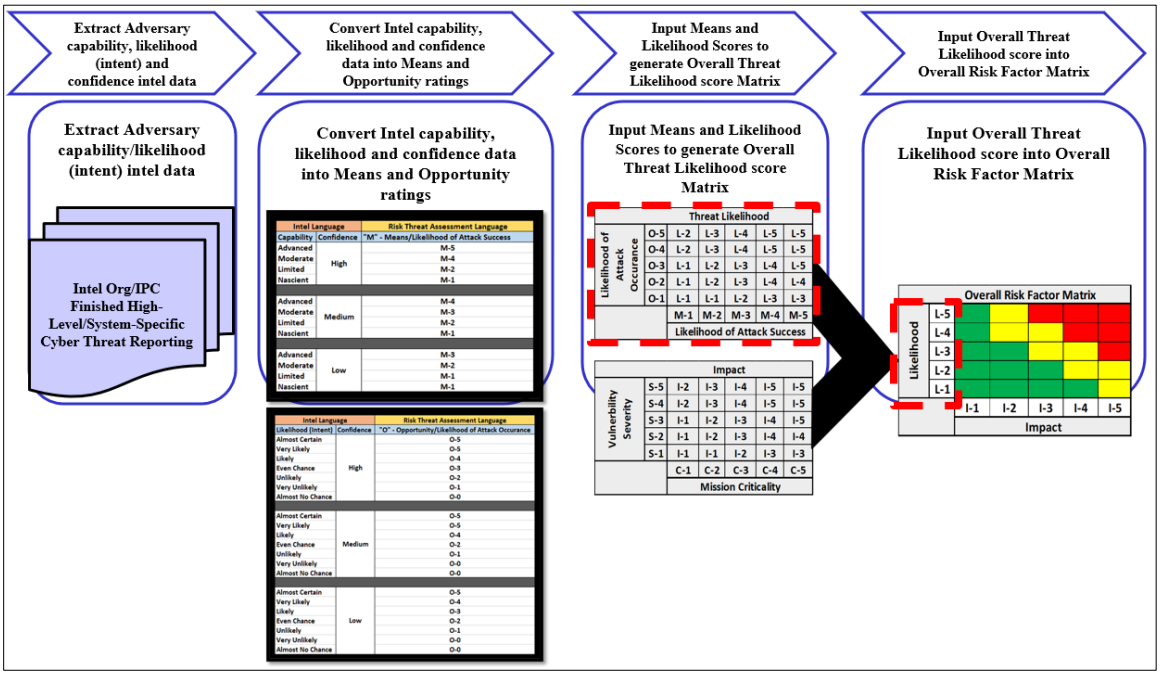
Figure D-3 displays typical risk matrices used for test events.



Source: U.S. Air Force 48th Cyberspace Test Squadron

Figure D-3. Example Risk-Level Matrices

Threat likelihood provides only half the required scoring to determine the overall risk posed by cyber threat susceptibilities/vulnerabilities discovered during test events. The IC calculates the threat likelihood scoring by converting capability, intent, and confidence intelligence assessment reporting language into "means and opportunity" threat ratings. Figure D-4 displays a flowchart highlighting an example of an intelligence unit process for conducting this conversion.



Source: U.S. Air Force 48th Cyberspace Test Squadron

Figure D-4. Example Intelligence Language to Risk Language Conversion Flowchart

D.8 Points of Contact

Points of contact (POCs) for cyber threat information include the Acquisition Intelligence Support Working Group (AISWG) and DCSA:

- The AISWG meets to identify and discuss issues relevant to the acquisition of intelligence threat support throughout all stages of the acquisition process. AISWG members include Service intelligence staff, the acquisition community, the testing community, the requirements development community, and the Defense Intelligence All-Source Analysis Enterprise. For more information, see the Intelink page: https://intellipedia.intelink.gov/wiki/Acquisition_Intelligence_Support_Working_Group.
- DCSA Website: https://www.dcsa.mil/.

Appendix E: Attack Surface Characterization

E.1 Purpose

This appendix includes supporting activities to identify and analyze the attack surface to understand the cyber risk to the system relative to mission operations. The goal is to understand how the system design, system components, interfaces, supporting technologies, and networks may create attack opportunities for cyber adversaries. This analysis helps the CyWG and cyber test teams to scope testing; inform MBCRAs (see Appendix G:); establish test objectives, timelines, and priorities; and plan for specialized test teams, infrastructure, required test articles, tools, instrumentation, and data collection.

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).

Conducting an attack surface analysis is an *Iterative Planning for Cyber DT&E* process to:

- Inform:
  - System design and operation to eliminate or mitigate identified architecture susceptibilities.
  - Risk of potential mission impact from cyber faults.
  - Test planning and prioritization to evaluate whether vulnerabilities are reachable and exploitable and whether there is an explicit path from potential exploits/faults to mission failures.
  - Cyber T&E requirements for government and system developer test activities, tools, and facilities.
- Identify system responses to adverse conditions (fail open or fail closed, repair or discard malformed data, etc.) and performance in backup modes.

Initial attack surface activities may be based on mostly functional information (e.g., all system details may not yet be available), and subsequent *Iterative Planning for Cyber DT&E* activities and tasks improve and clarify the activities and supporting activities described in Section E.2 to improve the overall analysis outcome. Careful use of automation, whether in defining input artifacts, analyzing exploit paths, or cataloging and linking analytical outputs, may expedite and facilitate this effort, enabling repeatability and improving accuracy. See the tools listed in JETEP under the Cyber T&E group: https://jetep.apps.dso.mil/cyber_te.

E.2 Identify the Attack Surface

The CyWG should consider all possible aspects of the attack surface, as represented by the wheel of access example in Figure E-1.

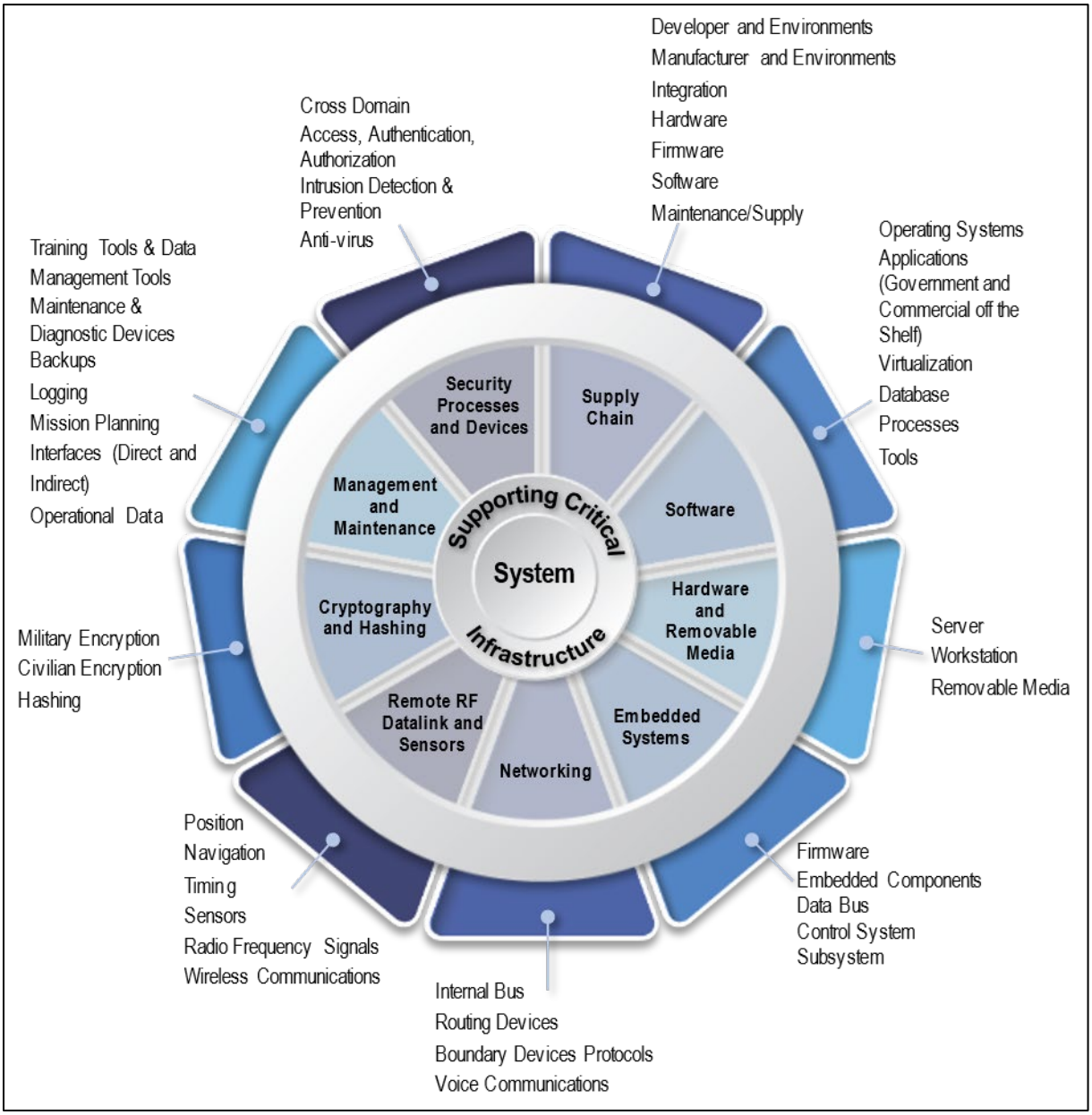


Figure E-1. Wheel of Access

Action 1: Examine System Architecture, Components, and Dataflows

- Examine available design artifacts, drawings, and diagrams (or models if using MBSE) and validate the functional relationships, trust boundaries within the system under examination, and tolerance/resilience properties of the functional architectures.
- Analyze systems implementation artifacts and validate dataflows and types, external/ internal interface ports, hardware and software inventory, and classification boundaries. Include maintenance and support equipment allocated to the system such as an aircraft test kit or propulsion maintenance devices.
- Identify all forms of communication, network connectivity, software, hardware, ICT supply chain, and human interaction.
- Decompose the system architecture, components, and dataflows to reveal the interfacing systems and data connections. Current best practice is to use systems control theory to illuminate control flows and highlight dependencies.
- Identify all points of entry/exit into the system by examining any external interactions including hardware, software, or firmware, even if limited or temporary.
- Summarize the attack surface details in an attack surface list of components, interfacing systems, and dataflows for further analyses; as more system details are known, iterate through Action 1 to update the attack surface details.

Action 2: Examine List of Previously Identified and Current or New Vulnerabilities and Exposures

Review:

- The NVD and CVEs, comparing them to current software, firmware, and hardware information.
- Any previous test results for unresolved vulnerabilities and exposures in the system.
- Known ICT supply chain security risks and breaches relevant to the system and components. Contact the NCIJTF for further information at the appropriate classification levels.
- Available threat assessment information to identify and better understand potential attack vectors used by adversaries.
- Threats or TTPs used against similar systems to help teams understand the expectations against the system.

Action 3: Examine Expanding Attack Surfaces

The CyWG should explore emerging elements that may be part of the system under development. Not all elements discussed below apply to all systems, and not every cyber DT&E approach requires consideration of every technical area. This list expands on Table 1 (Examples of Evolving Attack Surface Elements) in DoWM 5000.103 and is not comprehensive.

Additive and Computer-Aided Manufacturing

Additive and computer-aided manufacturing systems produce system parts using digital data instead of traditional engineering measurements and specifications. The digital data are vulnerable to attack, which may result in the production of substandard parts that are difficult to surface during testing.

- Identify:
  - Sources of information directly used to produce system parts to understand the unique risks for program managers using this technology.
  - How data corruption can occur and lead to failures in critical, mission-essential components.
  - AI (e.g., machine learning, deep learning, natural language processing, robotics); AI software is nondeterministic. AI is an emerging field for cyber threats. Include AI capabilities to defend the system.
    - Consider access to training, models, and model parameter data.
    - Review and consider MITRE ATLAS™ matrix techniques (https://atlas.mitre.org).
    - For more information, consult the online interactive Appendix M (currently under development).

Big Data Applications

A big data application is a software application designed to handle and analyze large, complex datasets beyond the capacity of traditional databases and data processing systems. Because of the large volumes of sensitive data that these applications handle and the distributed nature of their architecture:

- Examine:
  - Access controls, the use or lack of encryption, configurations for firewalls, intrusion detection and prevention, patching frequency, and processes.
  - Architecture and interfaces.
  - Commercial cloud environments and cloud services; consult Appendix H:.

- The DIB; data exfiltration and ICT SCRM practices pose ongoing risks to the systems developed by the DIB.
- Supplier performance risk reports, if available.
- PPIPs for ICT SCRM approaches.
- Available Cybersecurity Maturity Model Certification (CMMC) data.
    - Use ICT supply chain illumination tools to routinely characterize various supplier-related risks.

Defensive Cyber Systems

Defensive cyber systems are part of the system's attack surface, giving direct and indirect access to systems through trusted channels as a part of monitoring activities. Identify DCO monitoring and detection tools as a component of the system's attack surface. Exploited DCO tools may compromise system security through a trusted path.

DoW Infrastructure and Enterprise Services

The system may depend upon interfaces with external infrastructures and services. Examine trust relationships, access, identity, and access management.

Expanded Attack Surfaces

Expanded attack surfaces include potential side-channel vulnerabilities (ultrasound, differential power analysis, Ethernet over Power, Power over Ethernet, etc.); electronic components that store data from buses and pass data between components; and interfaces used for administrative, maintenance, or debugging purposes.

Examine:

- Every system-connected component (permanent or temporary), including cross-domain solutions; test equipment; maintenance devices; and digital data creation, storage, and transfer devices or processes.
- Trusted interfaces with both internal and external systems as part of a system's attack surface to expose communications vulnerabilities, including denial-of-service attacks that might disrupt or degrade mission performance.

Electromagnetic Spectrum, Cyber-Electronic Warfare Interfaces

Cyber/EW interfaces are potential paths for generating faults within a system. Cyber/EW attacks may exploit inherent subsystem properties to defeat components of the system or to get past the analog-to-digital converters in the system and achieve execution space within the

victim. The antennas and processing chains are therefore part of a system's attack surface. Appendix L contains additional information.

- Examine any wired and unwired interfaces to system components including intermediary system RF interfaces such as weapons connected to the MIL-STD-1553 data bus with external Global Positioning System (GPS) connections and software-defined radios with GPS connections.
- Determine whether the antenna processing chain is using Harvard or von Neumann architecture. Provable strict Harvard architectures are very resistant to allowing execution within the A/D boundary and are a lower overall cyber risk.

ICT Supply Chain Interactions

ICT supply chains supplying the hardware and software of the system under development contribute to a system's attack surface.

- Examine:
  - Contractual language is necessary to support conducting this essential exploration and to ensure that the government test community has access to ICT supply chain illumination details.
  - Software, firmware, and all available hardware, firmware, and software BOMs to identify ICT supply chain vulnerabilities and areas of unknown risk.
    - Review mission functionality to understand both critical and non-critical components.
    - For more information about ICT supply chain threats and risks, refer to Appendix F:.

Inter- and Intra-System Architecture Network Interfaces

All system architectures using networking technology contain well-known attack vectors.

- Review the network technology that the system will use; include both DoW networks and non-DoW networks, industrial control networks common on ships and aircraft, vehicular networks, networks local to the system, and non-IP networks (e.g., MIL-STD-1553).
- Analyze dependencies on interfaces to supporting or underlying infrastructure, including U.S. critical infrastructure (e.g., power grid).
- Note any mission or survivability risks due to the critical infrastructure dependencies.

Interfaces with Interagency

Consider all government sources (e.g., Defense Intelligence Enterprise, DITL, Central Intelligence Agency, Federal Bureau of Investigation, Department of Energy, Department of Homeland Security, CISA).

Microelectronics and Hardware Assurance

Hardware assurance depends on secure system design practices, development, procurement, and assembly tools and processes.

- Review:
  - Any commodity and/or COTS components incorporated into the system design that could introduce attack vectors.
  - System development activities to uncover vulnerabilities, their risks, and potential mitigations throughout the hardware life cycle.
    - Obtain available cyber intelligence reports for any embedded hardware technology.

Offensive Cyber Systems

Offensive cyber systems operate in a contested cyberspace to achieve direct effects on adversary systems and capabilities.

Examine:

- Detectability, attribution, and "coopt-ability" of these systems to determine risk. For more information, refer to DoDI O-3600.03, "Test and Evaluation of Cyberspace Effects and Enabling Capabilities."
- System interoperability in contested cyberspace because these systems access and communicate with adversary systems.

Real-Time, Safety-Critical Systems

Examples include industrial control systems and supervisory control and data acquisition systems. DoW weapon systems, critical infrastructure, and platforms usually include embedded cyber physical components that are either COTS or proprietary, and the unique protocols involved are often available in open source. See Appendix L for additional information.

Examine:

- The access vectors and ICT supply chains for these systems.
- Open-source reporting on COTS components.

Recovery and Restoration

Systems should have the ability to protect critical functions and restore needed mission capabilities within the required mission timeframes when an attack occurs.

- Examine the mission's tolerance for downtime and degraded operations.
- Investigate developer forensic capabilities to understand attacks, mitigate the impacted system or component, and prevent reoccurrence.

Software Assurance

Software to consider includes contracted software services (e.g., SaaS), developed software, OSS, firmware, and COTS, which all depend on the security of the software development facility, tools, and processes.

- Inspect and analyze software design for unintentional or intentionally inserted vulnerabilities (including previously known vulnerabilities), including common types of vulnerabilities (e.g., Open Worldwide Application Security Project (OWASP) Top 10, CWE Top 25).

Software Factories

Contractor and government development facilities are part of any system's attack surface via the development environment, tools, processes, and staff. Software factories include government and contractor owned or operated facilities.

- Examine software libraries, open-source code, software tools, and automated scripts in use by the government or contractor development team that may contain malware.
- Review:
  - Development personnel practices for vetting software coders and engineers.
  - Planned or current contractor or government development and test environments (tools, processes, staff) for vulnerable components.

System Architecture and Design Choices

Architecture and design choices are part of a system's attack surface and may introduce inherent risk that is difficult to resolve after system development.

Examine:

- Data inputs and outputs including points where data encryption, decryption, inspection, manipulation, storage, and sharing occurs.

- Embedded systems; control systems; and hull, mechanical, and electrical systems that are part of the overall SoS architecture.

Action 4: Analyze and Decompose System Mission

If mission decomposition has not already been performed as part of criticality analysis, integrate with the SSE team and perform an end-to-end mission and functional decomposition. The results of an attack surface analysis clarify what information flows in and out of a boundary.

- Review:
  - The system CONOPS and additional systems documentation to analyze the mission execution parameters and timeframes for mission accomplishment.
  - The DCO and maintenance processes for potential additional attack surface entry points.
- Identify:
  - Mission- and safety-critical functions and system recovery and restoration/adaptability requirements supporting mission operations.
  - System operator, defender, and system administrator roles and responsibilities and their intersection with mission-critical functions.
- Update the attack surface listing with potential insider/near-sider attack surface points based on internal protections, and identify all human interaction with hardware, software, and firmware.
- Decompose the mission down to the specific applications, the functions within those applications, line-replaceable units, and third-party libraries.

Best Practice: Air Force Functional Thread Analysis

As a component of the U.S. Air Force Mission-Based Risk Assessment Process for Cyber, the functional thread analysis enables a consistent approach to functional and mission decomposition with attack surface analysis. For more information, go to https://go.intelink.gov/MRAPC.

Action 5: Map Mission Dependencies

As with Action 4 (Analyze and Decompose System Mission), perform mission dependency mapping if it has not already been completed as part of a criticality analysis. Mission dependencies will extend and contextualize the results of Action 1 (Examine System Architecture, Components, and Dataflows).

- Use the PPP or other 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.
- Look for interdependencies of critical functionality on non-critical components and identify additional areas in the ICT supply chain not previously considered critical.
- Use the mission dependency mapping to develop an approach to verify system recovery and restoration requirements.
- Develop a criticality overlay on the mission dependency mapping and the attack surface list to use in the next activity. The overlay should clearly identify the following items in the attack surface list:
  - Mission- and safety-critical functions.
  - Critical functions, components, and information flows designated as key cyber terrain.
- Document the attack surface examination using a list or diagram relating system missions, mission- and safety-critical functions, components, communication paths, attack paths, designed-in dependencies, and mission-essential nodes or exposures.

E.3 Inform MBCRA

Prioritize areas of the attack surface for testing based on the mission risk including mission impact and threat characterization. The CyWG should use the attack surface characterization to inform each MBCRA (see Appendix G:).

Appendix F: ICT Supply Chain Cyber DT&E Considerations

F.1 Background

> **C-SCRM**
>
> C-SCRM manages the risk that a person or group could sabotage, maliciously introduce an unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an ICT item of supply, service, or system to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such a service or system.
>
> See the CISA ICT Supply Chain Resource Library at https://www.cisa.gov/ict-supply-chain-resource-library

Cyber DT&E by either the system developer or the government can help identify and mitigate threats to a system's ICT supply chain associated with the unique attributes of ICT supply chains. SCRM, under the SSE discipline and in accordance with DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," minimizes ICT supply chain and engineering risks to the DoW's warfighting capabilities, business systems, and enterprise information systems to maintain a technological advantage. DoDI 5200.44 specifies the responsibilities for implementing ICT supply chain requirements and states that DoW will manage risk to the assurance of systems throughout the entire life cycle as part of TSN processes, tools, and techniques to "assess vulnerabilities in custom and commodity hardware and software through thorough use of test and evaluation capabilities, including developmental, acceptance, and operational testing." The system developer is responsible for implementing countermeasures to thwart adversaries from exploiting the ICT supply chain. This appendix provides considerations for supporting countermeasure verification using cyber DT&E.

ICT supply chains can be complex and vast, including many tiers of global, interrelated designers, manufacturers, and logistics elements, which results in complicated corresponding attack surfaces. ICT supply chain risks exist not only for the system's hardware and software components but also for their development (e.g., software factories, manufacturing lines), production, and test environments (including processes, tools, and data). Additionally, ICT supply chains continuously evolve because of market forces on suppliers, including complete disruption in the event of wars or pandemics.

ICT supply chain vulnerabilities can emerge at any point during the acquisition life cycle of a system, from initial research to the design, development, production, transport, storage, maintenance, and disposal of the system. ICT supply chain attacks are more difficult to detect and can be more sophisticated than traditional cyberspace attacks. For example, any adversary ICT supply chain attack either needs a set of triggers to operate autonomously or requires an active command/control path from the adversary to the victim. Any non-malicious ICT supply

chain threat actors likewise need the right set of inputs for discovery. Unless explicitly restricted, the potential state space and attack surfaces for modern systems are unlimited.

Compromises to the system may:

- Already be present at the time of testing and actively evade detection.
- Lay dormant with no observable behavior until activated (perhaps autonomously).
- Occur in any part of the system, including in non-critical parts facilitating the compromise of critical parts.
- Originate through routine software, firmware, or hardware updates.
- Involve:
  - Complex interactions between hardware, software, and firmware.
  - Threats not previously known to the IC.
- Result from the compromise of trusted suppliers, especially via attacks by advanced threat actors.

CyWGs should use the concepts in this appendix to understand the cyber risk to mission- and safety-critical functions arising from these ICT supply chain attributes. This insight may lead to enhanced ICT supply chain countermeasure verification or unique adversarial objectives targeting potential ICT supply chain exposures during cyber DT&E. This appendix expands beyond the software supply chain focus of Executive Order 14028, "Improving the Nation's Cybersecurity," to consider cyber DT&E for software, firmware, and hardware supply chains.

F.2 ICT Supply Chain Cyber Risk and Cyber DT&E

The CyWG should consider ICT supply chain risks throughout the cyber DT&E process and should review available information in the system developer's SCRM Plans. The following subsections provide specific considerations for each of the cyber DT&E process activities for the ICT supply chain, expanding on the material presented in Sections 3 through 7.

F.2.1 Continuous Planning Considerations

As part of the continuous *Planning* activities, the CyWG should:

- Obtain regular ICT supply chain illuminations and review the SCRM countermeasures in the PPP and PPIP from the program protection team, if available.

- Review and provide input for contractual language, using the example guidance in Appendix I: and the details in Section F.2.1.6, to ensure that countermeasure verification includes cyber DT&E, where appropriate.
- Review available ICT supply chain threat characterization. See Section D.6 in Appendix D: for information on requesting intelligence assessment support for C-SCRM.
- Analyze all available BOMs, including a review of any SBOM continuous monitoring practices and VEX assertions.
- Include the ICT supply chain in the attack surface characterization (see Appendix E:) informed by criticality analysis (e.g., from the PPP).
- Evaluate potential risks during MBCRAs.

VEX

VEX is a framework designed to facilitate the efficient exchange of information on vulnerabilities and their exploitability. VEX assertions can provide valuable information directly from developers to enable effective triaging of vulnerability remediations.

Each of these activities provides insight for cyber DT&E. The CyWG should scrutinize these areas during the continuous *Planning* activities and be mindful of regulations, laws, and resources that often limit government test teams and the IC's ability to gather data from or about commercial sources. Program manager organizations should consider these intellectual property and proprietary restrictions and pursue mitigations when developing contractual language. The CyWG should request access to any program protection team tools (e.g., an ICT supply chain tool providing continuous assessments of risks in the ICT supply chain across all BOMs).

F.2.1.1 Threat Characterization

The SCRM lead should develop supplier threat assessment requests to the DIA SCRM-TAC based on the criticality analysis (see Appendix D:). For non-acquisition systems, the process may not be as clear. The SCRM-TAC provides supply chain threat assessment reports. See DoDI 5200.44 and DoDI O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," for more information.

The CyWG should coordinate with the SCRM lead and support the criticality analysis and countermeasure development. Threat characterization supports attack surface characterization and risk-aware test planning. The CyWG should carefully review supply chain threat assessments and periodically request updated threat assessments throughout the system's life cycle. See Appendix D: for more information on threat support for ICT supply chains.

When possible, program managers using the same suppliers or logistics entities, or who share similar systems or components, should share threat information with each other and with

government test teams. Public sources of counterfeit part data and any acquisition-community registries of part test information are valuable references for screening systems for known problems, such as checking non-critical system parts for which the CyWG may not otherwise plan rigorous system developer cyber DT&E.

Because complete ICT supply chain illumination may not be achievable for a complex ICT supply chain, the CyWG should endeavor not to limit threat characterization analyses to intelligence on known threats. Updating MBCRAs or using other forms of threat modeling, when the ICT supply chain or the system design changes, could identify potential threats to the ICT supply chain for which no intelligence warning exists. Threat modeling and emulation should prioritize risks with the greatest impact on the system's mission. The CyWG should routinely review the system design artifacts or digital models to identify exposures, exploited vulnerabilities, and avenues of attack through the ICT supply chain that an adversary may exploit.

F.2.1.2 ICT Supply Chain Illumination and Attack Surface Characterization

Illuminating the ICT supply chain is crucial for characterizing the attack surface it exposes. It also helps to identify:

- Relationships between elements of the ICT supply chain.
- Suppliers providing specific system components.
- CMMC levels of the relevant information system(s) used by the supplier(s).
- Foreign interests of suppliers, such as foreign-based ownership, controlling interests, partnerships, or R&D and manufacturing facilities.
- Design, development, test, and production processes and tools, including those used at system developer, developer, and government facilities.
- Security controls at system developer facilities.
- Procedures for the maintenance, storage, transport, and disposal of systems and components (including spares and software updates).
- Potential evolution of the ICT supply chain (including changes in suppliers).
- SBOM for each software component.

Government test teams should work closely with program managers and system developers to ensure that ICT supply chain illumination, implementation of security controls to manage ICT supply chain risk, and system developer testing are comprehensive. ICT supply chain illumination may require extensive resources and investments in illumination tools or platforms,

and MBCRAs can help determine the scope and depth of the illumination. The CyWG should focus on the critical ICT parts and suppliers with the greatest impact on the system's mission and obtain information on the provenance and role of most of the parts in the system to support risk-based screening and attack response.

ICT supply chain illumination provided by system developers may include:

- Detailed ICT supply chain maps.
- Documentation of system developer designs, policies, development processes, manufacturing and production processes (including part acceptance testing), disposal procedures, and security controls.
- Information on corporate, development, and production environments.
- BOMs, including HBOMs and SBOMs.

Existing artifacts may contain some of this knowledge (e.g., the PPP, PPIP), or the CyWG may need to seek specific contractual language provisions. Early in the life cycle, before a known list of suppliers is available for ICT supply chain illumination, criticality analysis, and attack surface characterization for subsequent cyber DT&E planning, the CyWG may need to rely on market research to identify likely suppliers or use the suppliers of similar, fielded systems as surrogates. The CyWG should update the attack surface characterization as the ICT supply chain evolves. If development is early enough before identifying suppliers, the CyWG should exert influence to ensure that requirements for illumination, provenance, testing and verification, and surveillance are included in budget estimates and in release documentation for system developers. System developers will appreciate having stable requirements and a contractual basis to enforce those requirements on their subcontractors.

Data Provenance

A detailed record of a product's origin, processing steps, and movement throughout the ICT supply chain, essentially tracking the "journey" of each component from its source to the final product, ensuring transparency and accountability in the process by documenting each transformation and transfer of data associated with the component, enabling verification of authenticity, quality, and compliance with regulations throughout the ICT supply chain.

The CyWG should assist with developing metrics for use in auditing the ICT supply chain through continuous monitoring techniques to minimize emerging risks due to an out-of-date PPP and PPIP. Continuous monitoring of software repositories (e.g., open-source code or software reuse) and automatic vulnerability resolution against the NVD will enable efficient patching of new vulnerabilities during software development and updates.

The review of detailed ICT supply chain test information and characterization of the ICT supply chain's attack surface require contractual language enabling test teams to form an integrated team with the system developer. This effort will likely require non-disclosure agreements.

Adversarial Supply Chain Risk Management Practitioner's Guide

For more information on the methods, tools, technologies, and processes that can assist in preventing the adversary from exploiting the ICT supply chain, contact the Air Force Life Cycle Management Center Armament Directorate.

The CyWG should revisit ICT supply chain risks recurringly throughout *Planning* to inform updates to the cyber DT&E strategy and when developing test plans during *Preparing* for individual T&E events. In this way, the CyWG can dynamically address changes in the threat, expected (or actual) mission environment, system design, and ICT supply chain on a risk-aware basis.

F.2.1.3 Hardware Assurance Considerations

Cyber test teams cannot easily test computer chips and printed circuit board assemblies acquired through microelectronics supply chains. The CyWG should become familiar with DoW hardware assurance testing capabilities (see the JETEP Website (https://jetep.apps.dso.mil/) for more information). The focus of this effort should be on critical components and subcomponents, or hardware associated with critical functionality. The CyWG should request specific information regarding a chip's design and manufacture to determine a minimum level of assurance for the product. The government may need to secure access to this information through contracts and non-disclosure agreements. When the government is acquiring custom or special-purpose chips such as application-specific integrated circuits, field-programmable gate arrays, and systems on a chip, the government needs assurance that the manufacturer performed certain tests appropriate to the chip and its intended purpose. Depending on the type of chip, the tests that the manufacturer may perform include:

Hardware Assurance Techniques

The WU Course, CYB 5610, "Cybersecurity & Resiliency for Weapons, Control and IT Systems" states that hardware assurance techniques include optical, acoustic, and X-ray microscopy, or even disassembly, delayering, and taking 50-gigabyte images of each layer.

- Passing of built-in test.
- Providing input stimulus to the integrated circuit and verifying its output.
- Verifying electrical characteristics (designed connectivity).
- Verifying thermal characteristics (heat and cold).
- Performing radiation exposure testing.
- Performing shake testing.

- Performing accelerated aging testing.

The CyWG should examine which tests the system developer performs (contractually or routinely) and ensure that the results aid the government in its evaluation of assurance for required performance and security characteristics of acquired chips.

Government testing may be necessary to address residual risk following system developer testing and risk mitigation efforts. The CyWG should coordinate with the program protection lead for opportunities to supplement system developer testing using unique government information (such as classified threat information) and specialized test resources and expertise. A government hardware assurance testing organization could spot-check or perform comprehensive testing as a strategy to manage unknown or unacceptable risks.

Minimally, the CyWG should verify, through contractual language, that printed circuit board designs are in accordance with the guidance provided by the DoW Executive Agent and DoDD 5101.18E, "DoD Executive Agent for Printed Circuit Board and Interconnect Technology."

F.2.1.4 Software Bill of Materials Data

In DevSecOps, process approval generally involves investigating the SBOM production process's implementation in a software factory. The CyWG will need either the tools involved in creating and analyzing SBOMs or access to the development team's software factory. A software factory should log SBOM-related events. Also, the process should produce an SBOM for the development environment and correlate the SBOM against a database of known vulnerabilities and VEX. The CyWG will conduct SBOM attribute analysis. Table F-1 provides a list of SBOM attributes from the National Telecommunications and Information Administration list of minimum SBOM elements.

Table F-1. Examples of SBOM Attribute Analysis

SBOM Attribute	Analysis	Possible Resulting Information	Cybersecurity Framework Category
Author of the software SBOM metadata	Service provider analysis	• Format used • Generation process used • Attributes identified • Analysis performed • Ability to share or distribute • SBOM integrity verification practice	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management
Supplier name of the components	Open-source analysis NCIJTF results	Supplier risk assessment	

SBOM Attribute	Analysis	Possible Resulting Information	Cybersecurity Framework Category
SBOM unique identifier	Integrity analysis	Use of a unique hash value to ensure immutable, auditable, and digital signatures for provenance	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management
Relationship of components	Dependency hierarchy	Relationship	
Complete software name Component software (direct dependency) Transitive dependencies (the direct component dependencies)	Dependency scan	• Count of all dependencies (direct and transitive) • Name of all dependencies	
	Vulnerability scan	Known vulnerabilities identified in the software	
	Technical debt analysis	• Number and degree of outdated dependencies whose vulnerabilities (known and potential) have long exposure times and create operational mission risk by making the capability challenging to update • Dependencies with no version number • Dependencies or components without an SBOM	
	Language scan	Number of programming languages detected within the software	
	Ecosystem risk	• Level of developer support • Supplier risk indicators such as end-of-life and change-of-control detection • Days since the last commit • Unique committers • Evidence of geographical origin	
Complete software name Component software (direct dependency) Transitive dependencies (the direct component dependencies)	License scan	Licenses for the project	
	Monitoring software (difference scan)	• Changes in the code detected since the previous five scans • Patterns of maintenance	
	Container analysis	• Container dependencies • Container images	
Component hash	Integrity analysis	Use of a unique hash value to ensure immutable, auditable, and digital signatures for provenance	

F.2.1.5 Input to the TEMP or T&E Strategy

The cyber DT&E strategy should include risk reduction plans for ICT supply chain risk. Planned activities should include MBCRAs, system developer cyber DT&E, government cyber DT&E, and risk mitigation efforts to expose and minimize cyber risk from the ICT supply chain. Test activities use MBCRA findings to focus on the areas of highest cyber risk to mission in the ICT supply chain. This approach, guided by criticality analysis, can improve the efficiency and effectiveness of ICT supply chain cyber DT&E.

Because of the size and complexity of the ICT supply chain, criticality analysis and risk assessment should inform planning the efficient and effective allocation of T&E resources toward the areas of highest cyber risk to mission. The risks may be associated with project or system data loss or system mission/capability impacts. The CyWG should plan cyber DT&E strategies to measure system surveillance, self-surveillance, resilience, and recovery to analyze the impacts of undetected ICT supply chain compromises where risks are either unknown or not mitigatable. The CyWG should consider adopting a perspective of "zero trust" for critical parts of the system by assuming prior and recurring supply chain compromises throughout the life cycle.

Deterrence

Cyber DT&E can provide deterrence against attacks on the ICT supply chain. Planning tests to uncover difficult-to-counter supply chain attacks and thus deny the adversary the benefits of those attacks may guide the adversary toward easier-to-counter attacks, easing the risk management challenge in the ICT supply chain. The discovery and attribution of ICT supply chain attacks also can support deterrence by facilitating the application of cost-imposing measures against the attacker.

The first layer of ICT supply chain defense comprises system developer testing and other security controls implemented by the contractors, developers, subcontractors, and logistics units.

The CyWG should plan for "active" test of the ICT supply chain if the contractual basis and requirements support the testing, particularly if the "reps and certs" (representations and certifications) section of the contract warrants that the parts provided are certified fit for a purpose (e.g., for car parts, there are certified parts attested as fit for a purpose, and there are junkyard parts that have no pedigree at all). When there is a requirement to mitigate or detect ICT supply chain compromises, test teams may intentionally inject supply chain faults and watch to see whether the system developer's surveillance and monitoring catches them. Where the system requirements specify that the system will be "fault tolerant," test teams may intentionally insert a known-bad part and verify that the system performs its mission regardless.

The TEMP or T&E strategy should describe the types of C-SCRM countermeasure verification in the cyber DT&E plan. The initial TEMP or T&E strategy should include an operational rationale for supply chain cyber DT&E requirements and the strategy for addressing ICT supply chain risk. Subsequent updates to the strategy should include the T&E techniques for each component of the system and a description of the resources required.

F.2.1.6 Contractual Considerations

In areas where the design is sensitive to the performance and quality of individual hardware and software components (i.e., where no requirement exists for fault tolerance), the government may choose to enforce C-SCRM requirements via contractual provisions, including the flow-down of cyber DT&E requirements to subcontractors. Specific DIDs for use in contracts are available in the DoW ASSIST database: DI-SESS-82433, "Cybersecurity Supply Chain Risk Management (C-SCRM) Software Bill of Material (SBOM) Requirements," and DI-SESS-82434 "Cybersecurity Supply Chain Risk Management Hardware Bill of Materials Requirement." Also see Appendix I: for contractual language considerations.

The CyWG should review the draft C-SCRM contractual requirements and provide additional recommendations, as appropriate. The CyWG should look for language such as:

- The system developer and its suppliers compile hardware and software BOMs and compare the BOMs to the actual systems delivered to the government.
    - These BOMs should be visible and auditable at each level of the design, "deeper" than the level of the delivered system, such as a handheld radio.
    - The BOMs should include backplanes, boards, controllers, interface cards, signal generators, configurable processors, etc.
- The system developer should plan for, and design test equipment and procedures used for acceptance to both screen for suspicious parts and perform automated checking for compromises.
- The system developer should plan acceptance testing to reduce ICT supply chain risk while balancing production efficiency with reducing later cyber testing demands.
- The system developer's acceptance testing should include auditable metrics through continuous BOM monitoring.
- The system developer compares subcontractor development and production environments against a known CVE list, VEX, and DoW Vulnerability Disclosure Program (VDP) data to identify parts at risk of compromise. The VDP can provide additional identification of production environment vulnerabilities.

- The software development pipeline employs automated checks to discover CWEs and CVEs through dynamic code reviews.
- Software development uses manual code reviews to identify probable attack vectors and infer exploitable flaws in system components.
- The system developer incorporates status and behavior monitoring in the system under development to identify anomalous behaviors more readily, including during performance testing.
- The system developer delivers verification of efforts to manage the complexity, scope, and dynamics of the ICT supply chain threat.
- The system developer will allow the government to use production facilities for planned cyber DT&E including access contractor or subcontractor development and test environments for inspections, security testing observations, or adversary emulation activities.

System developers may request explicit contract language to address responsibility for any damage to the system developer facilities caused by government testing; clarification of responsibilities when the government incidentally collects counterintelligence information or personally identifiable information; and access rights by government security personnel to ensure that the government test team did not leave government test tools behind in contractor or subcontractor development facilities after government testing.

State-of-the-Art Resources (SOAR)

Developed by the Institute for Defense Analyses, the 2016 SOAR study highlights a software assurance test planning process involving specifying technical security objectives. The CyWG should use the SOAR to determine which types of weaknesses need to be discovered based on criticality and risk. As an example, forced execution testing is the only test identified in the SOAR to find trojans. Forced path execution is expensive, requires specific expertise, and should be applied where there is greatest concern.

Test activities already specified in contracts, such as quality control testing, inspections, audits of software revision and inspection routines, and acceptance testing, may need expanded contract language to address the ICT supply chain explicitly. The government may request some of this language via a CDRL for the PPIP or specific system developer SCRM Plans, which the CyWG should review to avoid double or conflicting requirements.

The CyWG should ensure that Section L of RFPs (e.g., instructions, proposal preparation) requests that offerors provide information on:

- The mechanisms that the system developer has in place to monitor its ICT supply chain and implement countermeasures to mitigate risks, for example, use of NIST SP 800-161.
- How the system developer will meet ICT SCRM requirements.
- Supplier selection criteria for reducing ICT supply chain risks.
- How the system developer will protect ICT supply chain data and how the system developer will present ICT supply chain risk activities at technical reviews and major decision points.
- SBOM and continuous monitoring metrics.
- Continuous monitoring, regular testing, and flow-down of these requirements for development and test environments, processes, and tools (i.e., software factories, manufacturing lines).
- Integrity checking of the configuration management process and build process of software.
- Secure software development practice attestation.

Request and Reuse Data

The artifact and data repository should include results from system developer regular scans for known-compromised hardware and software within the systems and produced components. The CyWG should use the data to inform test planning.

The system developer's representations and certifications in the proposal should confer certain data rights that should show up in the contract. In some cases, this language is an assertion from the system developer about the fitness for purpose of the delivered system, under which the government can assert a right to verify. Expanded contract language (besides Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) provisions) may be necessary to enable effective government oversight of system developer activities and ensure that the government has sufficient data rights to continuous monitoring data and recurring third-party assessments.

The CyWG should monitor designs for all changes, usually as an expansion of normal diminishing manufacturing sources and material shortages surveillance, from the previous configuration and decide whether to recommend changes to the C-SCRM efforts. Changes indicating foreign ownership, control, or influence (FOCI) may be unavoidable, but the system developer should have processes to monitor for FOCI in its supply chain.

After delivery, regression testing could help identify whether changes in a system's behavior are outside what the engineering analysis and design anticipates for the declared design changes, a potential indicator of supply chain compromise between test events.

F.2.1.7 Continuous Planning Summary

The following list is a high-level summary for continuous planning for ICT supply chain cyber DT&E.

Continuous Planning (see Section 3)

- Review:
  - ICT SCRM requirements, including from:
    - DoDI 4140.01, "DoD Supply Chain Materiel Management Policy"
    - DoDI 4140.67, "DoD Counterfeit Prevention Policy"
    - DoDD 5200.47E, "Anti-Tamper (AT)"
    - DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage"
    - DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks"
    - DoDI 8500.01, "Cybersecurity"
    - DoDI 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers"
    - DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)" (now Part 117 of Title 32, Code of Federal Regulations)
  - C-SCRM plans and countermeasures:
    - PPP
    - SCRM Plan
    - PPIP
    - System developers' responses to RFPs
  - System developer hardware and software assurance testing results and other countermeasure verification.
  - Maps (e.g., relational diagrams) of the supply chain: software, firmware, and hardware parts, part producers, and part suppliers; storage, transport, and maintenance networks.
  - Relevant ICT supply chain threat information from intelligence and acquisition community sources.

  - ICT supply chain attack surface, especially for critical parts of the system.
  - Quality of data provenance for system components.
  - Software, hardware, and physical security controls throughout the supply chain.
  - Available manufacturer documentation on hardware tests performed and their results.
  - Evidence of manufacturer compliance with manufacturing standards for electronic components.
- Provide updates to the T&E strategy to address ICT supply chain testing:
  - Ensure that MBCRAs include ICT supply chain risk.
  - Ensure that government test teams have sufficient access to facilities, design information, and test information (including putting data rights in contracts). Ensure that the RFP provides guidance for how respondents should describe their proposed ICT supply chain T&E (see Appendix I:).
  - Prioritize ICT supply chain elements to test based on their mission criticality.
  - Ensure resources needed to support ICT supply chain T&E.
  - Provide contractual provisions enabling supply chain illumination, BOMs, and system developer and government cyber DT&E for ICT supply chain risk.

F.2.2 Preparing Considerations

If the test team will incorporate ICT supply chain scope in the test plan (see Section 4), the team may need specialized tools, techniques, and test personnel.

F.2.2.1 Documenting Test Plan Tools, Environments, and Techniques

Test teams should consider developing additional test tools to stimulate the system in atypical ways to try triggering dormant exploits (e.g., repeating tests with system time changes) and tools to simulate the effects of compromised system components to determine how the system responds and recovers. A test environment with a fully digital simulation of the system (a "digital twin") sophisticated enough to explore the system's response to a wide variety of potential attacks could greatly increase testable combinations of inputs and aid in test planning. These tests and simulations will complement those already contractually required of the system developer.

Some of the existing tools for testing hardware and software functionality, coding or manufacturing flaws, and the presence of malicious logic or hardware function irregularities include static and dynamic code analyzers, network monitoring tools, intrusion detection

systems, X-ray and acoustic systems for inspecting microelectronics, and optical systems for inspecting circuit boards.

The test team should consider consulting public and acquisition-community data sources on counterfeit and compromised parts or software (such as data from the Government–Industry Data Exchange Program and the Electronic Resellers Association International) to inform the choice of test techniques. The Supplier Performance Risk System (SPRS) provides a comprehensive view of a supplier's performance and risk profile. In addition, exclusion authorities provide a means to act upon unacceptable ICT supply chain risk levels. Examples of exclusion authority effects include the following:

Some SPRS Functions

- Assess supplier performance regarding the required quality standards.
- Identify potential risks associated with a supplier, such as financial instability, poor quality control, or noncompliance with regulatory requirements.
- Predict future performance.

- The authorities may limit or eliminate the exposure of DoD systems to the threats and vulnerabilities presented by the excluded supplier and/or the supplier's products.
- Some authorities combine with removal orders for products already integrated into DoW systems.

For storing and analyzing large amounts of data about complex systems' components and suppliers, test teams should consider using a common knowledge management system.

F.2.2.2 Identifying ICT Supply Chain Cyber DT&E Personnel

Cyber DT&E test personnel resources will be similar to those of other types of cyber DT&E. Personnel involved should have relevant knowledge of the ICT supply chain, ICT supply chain threats, and ICT supply chain risks. Test teams may also incorporate specialized supply chain threat SMEs and supply chain risk analysts. JETEP is a resource for hardware and software assurance assistance.

F.2.2.3 Preparing Summary

The following list is a high-level summary for preparing for ICT supply chain cyber DT&E.

Preparing (see Section 4)

- Describe the ICT supply chain test techniques, environments, and tools.
- Specify the personnel involved with ICT supply chain cyber DT&E.

- Describe the plans for ICT supply chain assessments on specified subcomponents, components, and subsystems.
- Describe the planned MBCRA and other ICT supply chain cyber test scenarios.

F.2.3 Considerations when Executing Cyber DT&E

See Section 5 for details on executing test events.

F.2.3.1 ICT Supply Chain Cyber DT&E Events

The CyWG should seek to observe the system developer ICT supply chain cyber test events, if contractual agreements support government observation. If required by the contract, the data repository may include data from independent contractor or developer tests; scans; and continuous monitoring of development, test, and production environments. The test teams should scrutinize all available data including SBOM continuous monitoring reports for OSS vulnerabilities and foreign- or adversary-developed code.

Test tools should stimulate the SUT in atypical ways to trigger implanted malicious code introduced by unknown threats and undetected ICT supply chain compromises. The test teams may need to "white card" tests to stimulate the specific system effects of an ICT supply chain compromise and then observe the mission effects or use M&S to predict system and mission effects. The Simulation Interoperability Standards Organization (SISO) Cyber Data Exchange Model can help reduce cyber manual testing to verify the effects from ICT supply chain compromises. In addition, the test teams should perform data exfiltration tests to ensure the confidentiality of data.

F.2.3.2 Executing Summary

Executing (see Section 5)

The following list is a high-level summary for executing ICT supply chain cyber DT&E:

- Use scans of the development, test, and production environments and tools for current patches and properly configured hardware, known vulnerabilities, known malware, and anomalous behavior.
- Test for the ability of the development, test, and production environments to detect potential compromises.
- Test to determine whether the development, test, and production environments (including processes and tools) satisfy requirements.

- Test to verify the performance of system developer acceptance tools.
- Test for counterfeit parts accepted by the production environment.
- Check for suspect parts in system copies (verify BoM accuracy, check part signatures, and validate checksums).
- Search for environmental triggers of hidden compromises by simulating inputs to the system in a laboratory environment.
- Check on system/subsystem/component/subcomponent behavior in a representative range environment using representative data exchange interfaces.
- Mimic attack behavior or effects in the system (e.g., "white card") to test system recovery and resilience.

F.2.4 Considerations for Evaluating Data

To evaluate the event, the test organization analyzes and interprets the data collected and then writes the event report. As with all other analysis, evaluate the test data against the requirements and test objectives in the test plan, and all data and reports should be available to any stakeholder in the data repository. See Section 6 for details on *Evaluating*.

Evaluating helps determine the sufficiency of the risk mitigations, considering evolving risks due to the changing ICT supply chain, threats, mitigations, and larger system design. Evaluations should inform iterative risk assessments of the ICT supply chain and continuous *Planning* for future tests. Ultimately, the evaluation informs a sense of the degree of trust afforded to the system (and its components and suppliers) and should inform the assessments of cyber resilience and operational resilience.

Evaluating (see Section 6)

Evaluating data from cyber DT&E focused on ICT supply chain includes:

- Tested MBCRA ICT supply chain scenarios; cross-check with test efforts and results.
- All records of unexpected system behavior to infer compromises.
- System developer test results.
- Data from government test activities, including the system's recovery and resilience to compromises.
- SBOM and OSS vulnerabilities in the system's software.
- Government test results.

- Whether tools for system developer's part acceptance testing are performing meaningful tests.
- Observed system behaviors.
- Identified areas of weakness in developer processes, tools, environments, and tools.
- Open-source vulnerabilities, checksum variances, effects of environmental triggers, and behaviors associated with ICT supply chain white cards.

F.2.5 Reporting Results

Reports should frame the evaluations of all data from T&E and other assessments in terms of cyber ICT supply chain risk and mitigation (see Section 7). Test teams should report all discovered vulnerabilities, compromises, and part test data to acquisition-community registries to allow other system development efforts to benefit from this information.

Reporting (see Section 7)

Reporting on ICT supply chain cyber DT&E includes:

- ICT cyber supply chain DT&E findings, including identified risks.
- Observed anomalies in the system, subsystem, component, or subcomponent.
- Part test data (to acquisition community registries).
- Confirmed or disproven MBCRA supply chain scenarios.
- All unexpected system behaviors.
- Evaluated areas of weakness in developer processes, tools, and environments.
- Identified open-source vulnerabilities, checksum variances, effects of environmental triggers, and behaviors associated with ICT supply chain white cards.

F.3 Iterate Cyber DT&E Activities

The CyWG iterates the cyber DT&E activities (*Planning, Preparing, Executing, Evaluating*, and *Reporting*) to ensure that updates to the threat and the tracking of new vulnerabilities continuously inform cyber DT&E efforts and ICT supply chain risk.

Appendix G: Mission Based Cyber Risk Assessments

This appendix expands upon MBCRA expectations stated in DoWM 5000.103 and throughout this guidebook. An MBCRA is an analytical iterative process to identify, estimate, assess, and prioritize risks to DoW operational missions resulting from cyber events. Regardless of the S&T effort, AAF pathway, development strategy, or deployment strategy, the system development artifacts and planning documents should address MBCRAs throughout the life cycle. MBCRAs should inform decisions associated with engineering, transition (to warfighter, POR), knowledge points or milestones, risk management, T&E, defensive TTPs, and operational utilization activities. Each MBCRA should update previously generated MBCRA products to incorporate test results and changes in the design, environment, mission, and threats, providing internal and external stakeholders with actionable information. Stakeholders may include program managers, project engineers, S&T managers, the system developer, the SE team, the SSE team, the information systems security manager (ISSM), T&E personnel (DT&E and OT&E), operational users, system defenders, system maintainers, functional sponsors, and any other desired stakeholders. This appendix provides guidance on required MBCRA elements and the use of MBCRA results in SE, cyber T&E, risk management, and intelligence.

The CyWG can use this overarching MBCRA guidance as a stand-alone or in conjunction with a specific published methodology (e.g., Cyber Table Top, Mission-Based Risk Assessment Process for Cyber, Cyber Survivability Risk Assessment). The CyWG can accomplish each of the critical MBCRA elements sequentially or concurrently. If the selected methodology does not include all the minimum elements in DoWM 5000.103 then the CyWG should supplement the selected methodology with the missing elements.

WU MBCRA Training

CYB 5630V: Two-and-a-half-day virtual course for the DoW Cyber Table Top methodology.

CYB 0090: Under development as a part of the WU Cyber T&E Foundational Credential.

G.1 MBCRA Critical Elements

The MBCRA will incorporate the critical elements depicted in Figure G-1 and detailed in this section using tables. The follow-on sections of this appendix provide additional information for each critical element. DoW Component-level guidance may provide additional information.



Source: DoWM 5000.103

Figure G-1. MBCRA Critical Elements

G.1.1 Input: Review Artifacts

Table G-1describes the MBCRA Input element. Unless otherwise stated, the MBCRA team performs the activities in the table.

Table G-1. Input Element

INPUT (Review Artifacts)
• Primary inputs include operational mission information, system documentation, previous test and evaluation (T&E) results, threat assessments, criticality analysis results, and cyberspace attack surface characterization products. • Ensure that all inputs are current and reflect the latest available information.

INPUT (Review Artifacts)
• If the program manager's organization did not previously conduct a threat characterization, cyberspace attack surface characterization, and criticality analysis, the CyWG should plan to accomplish each before starting the assessment or as part of the MBCRA itself.
Operational Missions
• Includes: – Understanding of the system's primary and secondary missions, mission-critical functions, safety-critical functions. – Threads/operational tasks: Specific scenarios or steps outlined to complete the mission(s) (CONOPS, CONEMPs, DoD Architecture Framework products (e.g., operations activity model)).
Previous T&E Results
• Review previous cyber test results to understand the vulnerabilities potentially applicable to the SUT. – Consider previously identified cyberspace attack paths. – Consider prior evaluations of systems or components in surrogate or legacy systems.
System Documentation
• Review all applicable system documentation to inform the MBCRA. Appendix C: has an example of typical documentation. – Consider the need for non-disclosure agreements. – Consider document transfer processes for dissimilar information systems. • Do not delay until additional information is available or the documents are more mature. • If system documentation is not available, use documentation for a similar/surrogate system to understand legacy system weaknesses and vulnerabilities. – Consult similar/surrogate system program manager organizations for access to this documentation. • Consider assessment products as living documents and update them when more information becomes available. – Ensure that the system data repository includes new documents and updates when available.
Threat Assessment
• Review or request available intelligence and counterintelligence threat products including adversaries' means, capabilities, opportunities, tactics, motives, and intent. Refer to Appendix D: for additional information on requesting threat assessments. – If intelligence information is not available during MBCRA execution, consider updating the current MBCRA. • Use threat assessment products to understand the threat environment, adversary capabilities, previous cyberspace attacks, and preparations that adversaries have taken to inform potential attacks against the system. • Ensure products are current and reflect the latest available intelligence information. • Include supply chain and system vulnerabilities that adversaries have demonstrated a capacity/intent to exploit. • Consider insider and near-sider threats and recruiting.

INPUT (Review Artifacts)
Criticality Analysis
• S&T managers and program managers confirm that the system can perform critical functions to complete the supported mission(s) within the required timeframe(s) when faced with representative threats. – Associated critical data and dataflows are essential to executing critical functions (and the supported mission(s)) and thus become the initial cyberspace attack target set. • Review each mission, safety-critical function, and mission-critical function. • Review the list of assets and capabilities for each critical function related to primary and secondary missions. • Review critical data that are essential to the effective execution of each function. • Determine mission impacts due to the compromise of data confidentiality, integrity, and availability.
Cyberspace Attack Surface Characterization
• Review cyberspace attack surface characterization to identify potential threat vectors and entry points/dataflows that an adversary could exploit to gain access. Refer to Appendix E: for more details. – Examine available drawings and diagrams (or models if using model-based systems engineering), dataflows and data types, external/internal interfaces, hardware and software inventory, and other system-unique characteristics. – Review known vulnerabilities and risks. – Review available threat assessment information to identify and better understand potential cyberspace attack vectors used by adversaries. • Review tactics, techniques, and procedures used against similar systems.
The MBCRA process in this appendix is independent of the processes that generate the MBCRA inputs. These inputs are not exhaustive, and their absence could preclude the successful completion or usefulness of MBCRA results. Reminder: This guidebook contains generalized content.

G.1.2 Prepare: Shape Assessment

The primary activities involved in shaping the MBCRA include planning the assessment, selecting the methodology, deciding on the appropriate assessment timelines (see DoWM 5000.103), and tailoring the methodology to meet stakeholders' needs. The CyWG may accomplish the activities presented in this section sequentially or concurrently. Table G-2 describes the MBCRA Prepare element.

Table G-2. Prepare Element

PREPARE (Shape Assessment)
Planning
Begin planning for the MBCRA as soon as possible. Activities typically include gaining leadership support (for resources), scheduling, team building, defining scope and missions, and reviewing inputs.
Methodology
Use this guidance or select a formalized MBCRA methodology incorporating the critical MBCRA elements.
Timing
Schedule the MBCRA, taking into consideration the Adaptive Acquisition Framework pathway, development strategy, and deployment strategy. Plan sufficient time to complete the assessment and generate the resultant analysis products in time to inform the supported decision(s)/activity(ies), such as testing to validate the results.
Tailoring
Tailor the selected MBCRA methodology's activities and products as desired, ensuring that the effort addresses each of the critical MBCRA elements.

G.1.2.1 Planning Activities

Planning for the initial MBCRA should begin as soon as possible. Scheduling for subsequent MBCRAs should occur as early in the life cycle as possible with planning efforts beginning in sufficient time to support the planned assessment. The CyWG can complete the planning activities in any order or accomplish some activities simultaneously, when feasible. Table G-3 lists MCBRA planning activities and considerations.

Table G-3. Planning Activities

Planning Activities	Considerations
Secure leadership support	Obtain MBCRA support from the stakeholder responsible for affecting change. Typical changes may be: • Requirements • Design remediations • Mitigations • Engineering change proposals • Contracts • Test resources
Schedule the MBCRA	Schedule the MBCRA with sufficient time to inform decisions and activities, such as: • Requirements identification • Systems engineering technical reviews • ATO approval • Test readiness review • Cyber T&E • Sustainment

Planning Activities	Considerations
Identify stakeholders	Identify agencies/organizations with decision-making authority and those expected to use the MBCRA results, such as: • Program manager • OTA/OTO • LDTO • Participating or executing test organization • System developer • Intelligence • System operators/maintainers • Oversight organizations • Joint Interoperability Test Command • Cyber protection team • Safety community • Logistics/supply chain • Mission defense teams
Form the assessment team	Identify specific individuals from within the stakeholders who can contribute to the successful execution of the MBCRA. This may require: • Contract vehicles • S&T project, prototype, or acquisition program access/ read-in • Methodology training • System training • Establishment of key positions: – Process facilitator – Methodology/tool expert – Team leaders – Notetakers – Configuration manager
Identify a location	Select a location for the in-person event(s). Consider: • Assessment classification • Team size • Event duration • Facility capabilities/limitations • Travel requirements • Media requirements
Select operational missions	Identify operational missions within the scope. The criticality analysis mission decomposition effort, if conducted, should already define the operational missions.
Define the assessment scope	Determine which components, interfaces, and data exchanges are within the scope of the MBCRA. The assessment scope should balance the system scope with plans and objectives for follow-on DoW RMF activities and system developer or government integrated cyber T&E (see Section 1.6) and system-of-systems testing. The scope should include all anticipated or acquired logic-bearing components/systems, items requiring a new or updated ATO, and direct interfacing systems. The scope may expand to include a larger test scope depending upon the MBCRA objectives.
Create a data repository	Create or use an existing central data repository at the appropriate classification level and ensure that it is accessible to the entire integrated team. If using an existing repository, verify that the information is current and that new members have access. In many cases, the CyWG will use multiple data repositories at different classification levels. The data repository should remain the central storage location for current and future risk assessments, supporting documentation, and all related artifacts. Relevant system information typically includes a current list of

Planning Activities	Considerations
	requirements, system architecture, intelligence data, previous test results, and previous cyber risk assessment data. The MBCRA team lead should manage the repository(ies) in accordance with established configuration management policy and procedures.
Review artifacts	Review available documentation to understand the system and to support follow-on MBCRA analysis activities, including (at a minimum): • Cyber performance requirements • Architectural diagrams • Previous test results • Interface Control Document • Technology or program protection plan • Threat assessment • Cyberspace attack surface characterization • Criticality analysis • Vulnerability assessment(s) Assessments performed early in the acquisition life cycle may require a document review of legacy or surrogate systems. During document review, begin creating and tracking any request for information to resolve issues and enhance the analysis effort.
Conduct pre-event meetings	Before the in-person event(s), conduct meetings to ensure that the assessment team is sufficiently prepared to perform the planned activities.
Select a risk scoring methodology	Use a scoring method/rating scale from the selected MBCRA methodology for meeting stakeholder needs. NIST SP 800-30 also provides risk assessment guidance.

G.1.2.2 Methodology Selection Considerations

Choose a methodology (or combination of methodologies) to include the critical MBCRA elements as outlined in this appendix (at a minimum) and align with engineering, risk management, test, funding, and timeline status and needs. In some cases, the CyWG will need to execute the selected MBCRA methodology in conjunction with other engineering or analysis activities to generate the required data. Methodologies incorporate different levels of analysis fidelity, automation tools, and expertise requirements, which can impact the time and work level involved with executing the MBCRA. Table G-4. Methodology Selection Considerations provides some considerations when selecting a methodology.

Table G-4. Methodology Selection Considerations

Contributing Factor	Status	MBCRA Selection Consideration
Threat Assessment	Current threat assessment available	Select the methodology, building upon the previously conducted analysis.
	Not accomplished or requires an update	Perform or update the threat assessment and then perform the selected MBCRA or select a methodology

Contributing Factor	Status	MBCRA Selection Consideration
		that includes performing the threat assessment during the cyber risk assessment.
Criticality Analysis	Current criticality analysis available	Select the methodology, building upon the previously conducted analysis.
	Not accomplished or requires an update	Perform or update the criticality analysis and then perform the selected MBCRA, or select a methodology that includes performing mission decomposition, functional decomposition, and critical data identification as part of the assessment process.
Cyberspace Attack Surface Characterization	Current cyberspace attack surface characterization available	Select the methodology, building upon the previously conducted analysis.
	Not accomplished or requires an update	Perform or update the cyberspace attack surface characterization and then perform the selected MBCRA or select a methodology that includes performing the attack surface characterization as part of the assessment process.
Previously Conducted MBCRA	Previous MBCRA report available	Update the previously conducted MBCRA products using the same methodology as previously used or select a methodology ingesting previously conducted MBCRA analysis results.
	Not accomplished	Select the methodology with the activities and products aligning with system security engineering, risk management, and test needs.
Available Resources	Time	Select the methodology based on the time available to inform the objective decisions/activities.
	Financial	Select the methodology based on available financial resources.
	Personnel	Select the methodology based on available personnel and skillsets.

The CyWG should ensure that the MBCRA team incorporates the results of the latest cyberspace attack surface characterization, criticality analysis (e.g., mission and functional decomposition, critical data), and threat assessment. If the data were not available before executing the MBCRA, the CyWG may need to perform the activities, or the CyWG could select an MBCRA methodology that incorporates these activities.

The CyWG does not need to select the same MBCRA methodology throughout the life cycle. In some cases, the CyWG may wish to change MBCRA methodologies at various points in the acquisition life cycle to better align with the system's maturity and assessment product needs or use a combination of MBCRA and SSE methodologies to perform the required analysis activities

and generate the required MBCRA products. The CyWG should consult participating stakeholders before changing the selected MBCRA methodology to ensure that the new methodology meets stakeholder needs. The TEMP or T&E strategy, CSS, and integrated test schedule should specify the selected MBCRA methodology(ies), the planned execution schedule, the MBCRA planned objectives, and the follow-on T&E events to verify expected MBCRA findings.

G.1.2.3 Timing Considerations

Planning for MBCRA timing involves considering two categories: scheduling and iteration duration. MBCRA scheduling is largely dependent upon the system development and deployment strategies or acquisition pathway. Each assessment's duration will vary based upon several factors. The CyWG should consider both schedule and duration when planning and executing its assessments to maximize benefits.

The optimum time to schedule and conduct the initial/baseline assessment is as soon as possible, ideally before or while finalizing the cyber performance requirements. The CyWG should schedule subsequent assessment updates well enough in advance to adequately inform the supported knowledge points, decision(s), system requirements, design adjustments, test strategy development, risk mitigations, and test execution activities. Scheduling considerations should include:

- S&T project timelines.
- AAF pathway.
- Development strategy.
- Deployment strategy.
- SE review schedule.
- Cyber T&E schedule.

The CyWG should conduct MBCRA updates following changes in the system design, threat, cyberspace attack surface, operating environment, and missions and following cyber T&E events. The CyWG should conduct updates to inform the ATO approval process and capability enhancements. Review Section 5 of DoWM 5000.103 to understand the initial and updated MBCRA timing for each AAF pathway. Review "Cybersecurity in the Adaptive Acquisition Framework" guidance (found in the DoW CIO Library, https://dodcio.defense.gov/library/) to understand how the AAF, DoW RMF, and T&E processes and timelines interact.



The MBCRA duration is dependent upon how long it takes to prepare for and conduct in-person event(s) and generate the final report. Initial iterations and assessment updates performed during design reviews tend to take longer than updates performed at other times in the acquisition life cycle. Assessment duration factors include:

- Selected MBCRA methodology.
- Maturity of input artifacts.
- Tailoring considerations.
- Iteration number (baseline or update).
- Resource availability (personnel, facilities).
- Participation (personnel, expertise).
- Time dedicated to conduct the process.
- Automated tool availability.

Other factors impacting assessment duration include the system complexity; level of stakeholder involvement; selected MBCRA methodology tailoring; and changes made to the system, environment, threat, mission(s), and critical functions since the last assessment.

G.1.2.4 Tailoring Considerations

Tailoring an MBCRA involves increasing or decreasing the selected methodology's process or products. Adding steps, analysis activities, or products typically increases the assessment timeline while enhancing the assessment fidelity or product utility. Changing or removing steps or removing products, however, often results in reduced fidelity or product utility by the larger set of stakeholders.

Removing or reducing process steps may also inadvertently increase the assessment duration, complexity, and difficulty level as the reduction may result in the assessment team not reviewing or generating data needed later in the assessment process. To ensure that the executed assessments are successful and effective in informing the supported decision/activity, the MBCRA team should evaluate the process-tailoring activities against the potential costs and benefits of each adjustment. The CyWG should consult all stakeholders before tailoring or changing the selected MBCRA methodology (including the assessment products) to ensure that the MBCRA will still meet the stakeholder needs.

The CyWG should ensure that all MBCRA tailoring efforts still include all minimum elements in DoWM 5000.103 minimum elements. If the selected methodology does not include them, then

the CyWG is responsible for supplementing the selected methodology with the missing elements. Overarching tailoring guidance and considerations are provided (**in bold**) in the following subsections.

G.1.2.4.1 Define Assessment Scope

Limit the assessment scope. Limiting the scope to a small subset or subsystem of the larger system allows teams to focus their efforts and potentially accelerate assessments. However, this approach necessitates additional evaluations of the remaining subsystems and the overall SoS to ensure integration and interoperability. For example, concentrating solely on the assessment and authorization boundary to meet ATO approval requirements may reduce the workload, but it can also lead to the omission of critical operational details essential to the assessment. This narrowed approach may diminish the assessment's effectiveness and value for various stakeholders, including ITTs, mission defense teams, functional management offices, engineers, and developers. Moreover, it may decrease the likelihood of the assessment meeting the requirements outlined in Title 10, United States Code; DoW; and Service T&E guidelines.

Establish a scope to focus on a specific mission set(s). Limiting the assessment scope to focus on specific missions reduces the assessment workload and limits the assessment to only those parts of the system used to perform the critical functions associated with the selected mission(s). Although focusing on one mission will reduce the complexity, scope, resource requirements, and duration, it will also result in not analyzing some critical functions and aspects of the system for potential cyber vulnerabilities. The CyWG will need to analyze the remaining mission(s) and critical functions during follow-on MBCRAs.

Establish a scope to include all test assessment areas. Choosing an overall scope consistent with cyber test efforts ensures that the MBCRA meets T&E stakeholder requirements. If desired, the CyWG can perform multiple smaller, focused assessments on specific areas within the larger context or scope, meeting the exact needs of the upcoming supported decision/activity.

G.1.2.4.2 Review Documents

Gather a subset of documents required for the assessment iteration. Gathering a specific, yet inevitably incomplete, set of documents may take less time, but it increases the possibility of missing critical data and limits the team's understanding of the system.

Use draft documentation as opposed to waiting for final products. Using draft documentation could drive the team to make assumptions, potentially resulting in inaccurate assessment findings. However, waiting for final products could delay or prolong the assessment, significantly reducing potential assessment benefits. Using draft documents and updating the

analysis when more mature documents become available helps ensure that timely assessments are as current as the information available.

Use technical exchange meeting(s). Conducting technical exchange meetings before the collaborative wargaming event will help to reduce the time and personnel needed to conduct the event. This process allows the offensive team to plan and analyze attack paths before the discussion, allowing for more discussion time and fewer personnel resources used or needed to be available during the event.

Limit information (i.e., graphics, assumptions, intelligence). Decreasing the amount of information presented in a scenario reduces the workload and timelines, but it also diminishes the analysis and could skew cyberspace attack path and vulnerability analysis activities. The reduction in content also risks providing an insufficient amount of information to properly frame the scenario, thereby reducing the effectiveness of the analysis, including expressing potential risks of system implementation intentions and potential mission impacts of vulnerability exploitation.

Include a mapping of each cyberspace attack scenario to related cyber performance requirement(s). Mapping relevant cyber performance requirements will increase the workload. However, the mapping will also provide stakeholders with information pertaining to the planned cyber test events (if the MBCRA is informing the test) such as data collection to assess the effectiveness of cyber protection implementation. It also ensures that test events can inform the cyber performance measures and meet the test event objectives. These data can support *Iterative Planning for Cyber DT&E* and *Preparing for Cyber DT&E* activities and tasks.

G.1.3 Execute: Complete In-Person Event and Analysis

Table G-5 describes the MBCRA Execute element.

Table G-5. Execute Element

EXECUTE (Complete In-Person Event and Analysis)
Collaborative Wargaming (In-Person Event)
Conduct interactive discussions using adversarial cyber representatives, operators, and system design engineers, and, when available, defenders, developers, intelligence community representatives, and maintainers. Events provide an interactive environment to analyze the system, identify potential cyber risks, and develop recommendations to improve cybersecurity and cyber resilience. Typically executed in person, these events can take several forms, with the most common being a table-top exercise or a working group meeting. The table-top exercise normally includes an offensive team attempting to compromise the system and affect performance while the defensive team defends the system. It is important to

EXECUTE (Complete In-Person Event and Analysis)
capture all discussion points during the in-person event. Note takers should capture discussions by hand on paper, digitally using laptops, or using audio recording with transcribing capabilities.
Attack Path Analysis in Mission Context (In-Person Event or Analysis)
Using the attack surface characterization and criticality analysis, identify attack paths through specific mission-relevant terrain in a contested cyberspace that an adversary could use to progress from the attack surface, impacting mission- or safety-critical functions. Using the attack path analysis results, generate cyberspace attack scenarios to capture potential attack sequences, potential vulnerabilities along the attack paths, compromised target data, and resultant mission impact(s) in an operational mission context. The resultant cyberspace attack scenarios should include traceability to cyber performance requirements and articulate anticipated system behavior(s) of data compromises in contested cyberspace. During the analysis, the group should take into consideration the system's planned or implemented protections, such as cyber defenders; engineering workarounds; and operator tactics, techniques, and procedures.
Mission Risk Assessments (Analysis)
Using attack path analysis results and all relevant threat information, determine risk scores. Use a risk scoring methodology and adjust it as necessary to best meet the system development needs. Include, at a minimum, likelihood (e.g., potential vulnerabilities, threats) and mission impact (e.g., severity, criticality). Risk is a measure of the extent to which a potential circumstance or event can threaten an entity. It is typically a function of the adverse impact(s) arising if the circumstance or event occurs and the likelihood of occurrence. Mission risk assessments are subjective, resulting in qualitative factors for both impact and likelihood posing a mission risk. The assessed potential impact results from the compromise of one or multiple components of confidentiality, integrity, or availability, whereas likelihood addresses whether a threat can exploit a given potential vulnerability. There are many scoring methods available across DoW, and individual methodologies often have their own embedded scoring procedure or methodology. The CyWG should select a preferred risk scoring methodology and adjust it as necessary to best meet system development needs. Tailoring risk scoring can be based upon several factors, for example: • Level of fidelity. • Authorizing Official input. • Warfighter input. • Risk presentation approach. • Impact of data loss. • System performance. • Cyberspace attack cost. • Level of adversarial effort.

G.1.4 Output: Create Report/Out-Brief

Table G-6 describes the MBCRA Output element.

Table G-6. Output Element

OUTPUT **(Post-Event Analysis and Report Generation)**
• Primary outputs include risk analysis results, cyberspace attack scenarios, prioritized potential vulnerabilities, and recommendations captured in an MBCRA report and/or out-brief. • Create or update a MITRE D3FEND Cyber Attack-Defense (CAD) model of the cyberspace attack scenarios: – Ensure the selection of detailed and specific D3FEND classes on the nodes in the model. – Identify the known countermeasures and to which digital artifacts they are applied in the scenario. – Annotate the nodes in the diagram with essential information about the attack scenario. – Save and store the resulting D3FEND CAD model in a version-controlled repository. – Find additional documentation at this link: d3fend.mitre.org/cad/docs/. • Develop a MBCRA report (e.g., Power Point, Word document): – Provides stakeholders with actionable information to deliver a cyber survivable and operationally resilient system. – Becomes the living truth source to inform programmatic, transition, knowledge points risk management, engineering, test, defense, and operational decisions and activities. • Ensure delivery of the report to senior leaders and all members of the MBCRA team. Upload the report to the data repository (e.g., a digital environment such as Teams or Confluence). • Review and update the report during each subsequent MBCRA. • During sustainment, use the latest version of MBCRA products as the baseline for future upgrades.
Analysis Results
Summarize the assessment, including: • Scope, assessed missions, and critical functions. • Overarching assumptions and limitations impacting the assessment. • Findings and conclusions, including risk assessment results and identified high-interest areas. • Observations resulting in secondary or tertiary effects on other interfacing systems. • Cyberspace attack vectors, paths, protections, or scenarios requiring testing.
Cyberspace Attack Scenarios: Overview
Provide cyberspace attack scenarios for each mission-critical function (in scope) capturing potential and likely cyberspace attacks into and through the system, exploiting potential system weaknesses identified during the assessment, and targeting the identified critical data elements. Include, at a minimum: • Scenario-specific assumptions. • White cards used. • Access methods. • Cyberspace attack vectors and paths. • Targeted critical data and compromise type(s) (confidentiality, integrity, availability). • Expected impact on the system's ability to perform the critical function and resultant mission impact(s). • Scenario risk assessment result. • Areas of high interest to stakeholders.

OUTPUT (Post-Event Analysis and Report Generation)
• Test methodologies. • Anticipated test tools, environments, assets, and personnel. • Test risks, limitations, and mitigations.
Cyberspace Attack Scenarios: Critical Function Alignment
To ensure that the system can perform all critical functions in a representative threat environment, assessment teams should ensure that at least one scenario targets every critical function for completeness and adequacy and to inform scenario-based cyber T&E.
Cyberspace Attack Scenarios: Operational Mission Alignment
The assessment team creates scenarios using an operational mission context to illustrate system performance in a mission-relevant environment to articulate potential contested cyberspace events into and through the system, exploiting potential system weaknesses identified during the attack path analysis and targeting identified critical data elements and functions. Targeting non-critical data integrity or availability that can prevent critical data access at the place and time of need is sufficient to cause a significant mission effect and encapsulate the attack path analysis results and illustrate the potential impacts caused by data compromises in an operational mission context identified through the mission risk assessment. During scenario/vignette generation, it is important to consider the potential worst-case scenario as appropriate for the current configuration of the SUT. Without a significant impact, there is often little to no perceived risk to the system.
Cyberspace Attack Scenarios: Requirement Alignment
Once generated, each cyberspace attack scenario should help illustrate the potential risks created by the existing, proposed, or expected architecture and the requirements to inform follow-on risk remediations, mitigations, design decisions, and testing. The cyberspace attack scenarios should also be clear and easily understandable to senior stakeholders, who will eventually need to make decisions on actions to address the potential risks identified in the cyberspace attack scenarios. Linking system requirements with the scenario identifies test measures to improve the planning and execution of cyber T&E.
Cyberspace Attack Scenarios: Documenting for Reusability
Create or update a digital model of cyberspace attack scenarios aligned to the D3FEND cybersecurity ontology by executing the following actions: • Ensure the selection of detailed and specific D3FEND classes on the nodes in the model. • Identify the known countermeasures and to which digital artifacts they are applied in the scenario. • Annotate the nodes in the diagram with essential information about the attack scenario. • Save and store the resulting D3FEND CAD model in a version-controlled repository. • Find additional documentation at this link: https://d3fend.mitre.org/cad/docs/. **Sanitize scenarios for reusability across DoW** To support community reuse of attack scenarios, remove all specificity of attacks to the system and remove the mission impact context, then submit scenarios as controlled unclassified information instances to the OACRA Viewer, available on SIPRNET in the High Performance Computing Portal. For more information, contact OSDRE-DTEA-Cyber@groups.mail.mil.
Prioritized Potential Vulnerabilities
Identify prioritized potential (or actual) vulnerabilities and risks identified during the MBCRA either individually or as part of the generated cyberspace attack scenarios.

OUTPUT (Post-Event Analysis and Report Generation)
Recommendations
Provide a list of actionable recommendations for remediating or mitigating identified cyber risks/ vulnerabilities. Identifying more than one recommendation for potential risks provides program managers with multiple options for design and procedural improvements. Recommendations typically include: • New or adjusted cyber performance requirements. • Engineering change proposals. • Tactics, techniques, and procedures.

G.2 MBCRAs in Systems Engineering

The CyWG should plan MBCRAs to support SE efforts to ensure the integration of operational resilience into the foundational system design. MBCRAs can assist with developing robust cyber performance requirements, generating engineering change proposals when necessary, and informing M&S efforts. MBCRAs can also play a significant role in informing contract down-select efforts, design reviews, and other SE technical review efforts.

G.2.1 Cyber Performance Requirements

As the assessment team reviews artifacts, completes attack path analyses, and generates cyberspace attack scenarios, the team may identify missing or insufficient cyber performance requirements. Following an MBCRA, teams should make specific recommendations to improve requirements-driven performance (e.g., the system must detect unauthorized data written to the system). If the CyWG executes the MBCRA too late to impact system requirements, then assessment recommendations should focus on remediating or mitigating the risks.

Early Assessments

Because system requirements form the foundation of a successful system development, the cyber risk assessment team should conduct the MBCRA early enough in the life cycle to inform requirements before beginning the formal coordination process.

Early baselines enable rapid assessment updates to support time-sensitive decisions, knowledge points, and activities.

Measurable, testable, and achievable cyber performance requirements drive an engineering design to minimize or eliminate potential vulnerabilities identified by the assessment team. Review Appendix B: for further guidance.

The CyWG should consider using MBCRAs to advise on defining or updating cyber performance requirements when T&E verifies cyber vulnerabilities late in the life cycle or when similar deployed or future systems identify new cyber risks.

G.2.2 Engineering Change Proposals

MBCRAs may reveal potential risks associated with anticipated or proposed system designs and implementation strategies. When appropriate, the CyWG can propose recommended changes to the system's design, which may require engineering change proposals. These recommended changes should be clear and comprehensive to facilitate timely and effective implementation and will take one of two forms: remediations to design out the risk, or mitigations to reduce the risk of vulnerability exploitation or minimize the impact if exploitation occurs. Mitigations will not actually eliminate the risk. The CyWG should prioritize changes that design out, or remediate, the risk and improve performance whenever possible and should recommend mitigations when remediation of a potential or validated cyber vulnerability with mission-impacting risk or performance impacts is unaffordable or impossible. The engineering team should also look for opportunities to implement design changes that will eliminate or mitigate multiple cyber risks and cyberspace attack paths through the system. Subsequent MBCRAs should consider engineering changes made in response to recommendations and their effectiveness as risk mitigations.

G.2.3 Modeling and Simulation

The integration of MBCRAs and M&S can have a significant impact on the development and testing of systems. MBCRAs provide valuable insights into system characteristics, potential cyberspace attack vectors, and critical functions. This information enables modelers to develop M&S capabilities that can simulate system performance characteristics in the event of a cyberspace attack, allowing engineering and risk assessment teams to understand the anticipated system performance and the effectiveness of integrated cyber protections. By incorporating MBCRA results into M&S, teams can gain a deeper understanding of system interdependencies and potential vulnerabilities, ultimately informing the development of more effective cyber protections.

The effects of integrating MBCRAs and M&S are numerous. For example, M&S capabilities can support adversarial approaches in cyber DT&E, reducing the cost, risk, and scope of follow-on testing. Additionally, system security engineers can use MBCRA results to explore design concepts integrating or adjusting previously planned protections and remediating or mitigating potential cyber risks. By understanding stakeholder interest areas and intentions for follow-on testing, engineering teams can also incorporate targeted test capabilities into models, accelerating test opportunities and reducing the scope of follow-on test activities.

Lastly, M&S can also benefit from MBCRAs by leveraging simulated attacks in digital models to identify attack paths, vulnerabilities, and potential mission impacts. Using M&S can inform and improve MBCRAs by providing a more comprehensive understanding of system

vulnerabilities and potential risks. By combining MBCRAs and M&S, program managers can save time and money while improving system performance and operational resilience. Ultimately, the integration of MBCRAs and M&S can lead to more effective and efficient system development, testing, and deployment.

G.3 MBCRAs in Cyber DT&E

A significant benefit of conducting comprehensive MBCRAs is their role in scoping, prioritizing, and informing cyber DT&E by the system developer and the government. During the MBCRA, the assessment team identifies potential risk areas, nodes of interest, critical data, critical functions, and the potential mission impacts compromising a data element's confidentiality, integrity, or availability. This information informs test planning, preparation, and execution.

Sufficient time and resources typically do not exist to fully evaluate every potential system vulnerability and cyberspace attack path through the system. The MBCRA results should help inform (not limit) test activities. The MBCRA's cyberspace attack scenarios, coupled with the test recommendations captured in the report, inform cyber T&E planning, execution, and reporting. The scenarios capture the analysis results in an operational mission context and focus on the nodes and targets deemed of highest interest to the stakeholders. The cyber performance requirements, targets, and data compromise types identified during the MBCRA coupled with the anticipated system behaviors, potential cyber risks, test planning information, and cyberspace attack path information should create the foundation for the cyber test strategy, test resource list, test plan, and test report generation.

G.3.1 Developing the Cyber DT&E Strategy During Iterative Planning for Cyber DT&E

The MBCRA will identify specific areas of assessment for cyber DT&E such as cyberspace attack interfaces, key targets, and critical functions. MBCRA results provide insight into anticipated T&E resources and methodologies. This information helps develop a comprehensive cyber DT&E strategy and informs other documentation such as the SOW/SOO, PPP, TEMP or T&E strategy, and CSS. Table G-7 highlights key MBCRA attributes used to inform system documentation.

Table G-7. MBCRA Attribute Inputs to Documentation

		Documentation			
		SOW or SOO	PPP	TEMP or T&E Strategy	CSS
MBCRA Attributes	Mission Description			✓	✓
	System Description			✓	✓
	Key Interfaces/External Interfaces			✓	✓
	Critical Components, Critical Program Information, Critical Functions, and Critical Data		✓	✓	✓
	Potential Risks		✓		
	Key Capabilities (operational and/or technical)			✓	
	Threats			✓	✓
	Developmental Cyber T&E Approach	✓		✓	✓
	Test Resources	✓		✓	✓

G.3.1.1 Cyber DT&E Resources

MBCRA results help scope cyber DT&E resources. The resources needed to validate the MBCRA results may be listed in the MBCRA report, or the CyWG can derive the necessary resources from the details in the report. The MBCRA report should include the following resources for each area identified for testing: organizations, environment, assets, and tools. The MBCRA report may also specify unique test team expertise. In addition, the MBCRA report may discuss special data collection strategies, which may require new tools or instrumentation approaches. The CyWG should capture this information in the TEMP or T&E strategy. The information is also useful to the test team for determining funding and developing the team's detailed test plans and schedules.

G.3.2 Preparing for Cyber DT&E

The scope, objectives, and types of cyber testing will vary between non-acquisition, pre-acquisition, and acquisition programs. MBCRA results should inform the test plans during *Preparing for Cyber DT&E*.

Because MBCRAs and stakeholder inputs should inform testing, not limit it, cyber test organizations involved during *Preparing for Cyber DT&E* for upcoming testing should plan to address the MBCRA areas of interest and address meeting other required objectives. Cyber test plans should include a prioritized list of test activities and focus areas and a list of other areas (i.e., alternate cyberspace attack paths/nodes) that the test team will investigate if time and resources permit. The test plan should specify MBCRA-identified data compromises and the expected system behaviors. See Section 4 for additional test plan and preparation considerations.

As the system matures and the integration of subcomponents, components, and subsystems occurs, the system developer, the government, or an ITT should also review end-to-end MBCRA attack scenarios, implemented remediation, mitigations, and updated MBCRA results to determine the need to verify potential cyberspace attack paths through the system. The CyWG should consider the system's defense-in-depth posture and determine the system's overall cyber operational resilience performance.

Test Scope

The MBCRA provides a starting point for cyber test plan development, highlighting areas for consideration as part of a planned cyber test event, but it should not limit the overall scope of cyber testing. Test teams should always look at the areas identified by stakeholders but retain the opportunity to assess other areas of the system.

G.3.3 Evaluating Cyber Developmental Test Data and Reporting Cyber DT&E Results

MBCRA reports articulate areas identified for cyber DT&E and the anticipated mission effects of data compromises. Cyber DT&E (system developer and government) validates potential vulnerabilities previously identified during the MBCRA, finds new vulnerabilities, and assesses cyber resilience through the observation of system behaviors. During early cyber DT&E on subcomponents, components, or subsystems, the test team may not be able to validate all MBCRA-identified scenarios. Upon completion of such testing, the test team should compare validated vulnerabilities and resultant SUT behaviors with cyberspace attack scenarios generated during the MBCRA. The test teams may be able to deduce (using the documented inputs from MBCRA stakeholders) whether new remediations or mitigations are necessary and whether the scenario will put mission- or safety-critical functions at risk without those fixes. In cases where the test team successfully executed a full MBCRA scenario, the evaluation and report should articulate the actual impacts. The CyWG should compare test results to risk assessments to inform improvements to the MBCRA process.

Following hands-on cyber DT&E, the CyWG updates existing MBCRA products during the next MBCRA to incorporate validated vulnerabilities and behaviors observed during the test events. These updates are critical to ensuring robust follow-on cyber DT&E planning and execution; the prioritization of testing; the implementation of appropriate vulnerability remediations and mitigations; and the judicious application of limited test resources during follow-on test events. See Sections 6 and 7 for additional guidance on *Evaluating Cyber Developmental Test Data* and *Reporting Cyber DT&E Results*, respectively.

G.4 MBCRAs in Risk Management

MBCRAs enhance the S&T project, prototype, or program's larger risk management efforts, providing the data and rigor needed to inform the prioritization activities and complete the DoW RMF process. Understanding both the cyber risks present in a system and the



associated recommendations provided by the risk assessment team helps ensure the appropriate prioritization of risk recommendations. The MBCRA's attack path analysis, cyberspace attack scenarios, risk assessment, findings, and recommendation analysis activities directly inform the DoW RMF team's responsibility to integrate security, privacy, and cyber SCRM activities into the system development life cycle.

G.4.1 Recommendation Prioritization

The MBCRA report provides raw risk scores in an operational context, informed by stakeholder input, and risk mitigation recommendations for consideration. Understanding the potential mission impacts of vulnerability exploitation and the associated risk ratings and proposed mitigations can help risk management teams prioritize recommendations and maximize the utilization of limited program manager resources.

The raw risk score by itself is insufficient to prioritize the use of limited resources required to remediate or mitigate the vulnerabilities identified during the MBCRA. Program managers should consider raw risk scores in conjunction with other factors including:

- Secondary/tertiary effects of vulnerability compromise.
- Previous test results (if available).
- Stakeholder inputs.
- Illustrated cyberspace attack scenario effects.
- Recommendation cost analysis.
- Level of impact of recommendation implementation.

Using the combination of the raw score and other factors, the MBCRA team should prioritize each recommendation to address the potential vulnerabilities found during the assessment.

G.4.2 DoW RMF Assessment and Authorization



The risk management team should use the knowledge gained from the completed MBCRA to inform DoW RMF Assessment and Authorization. The risk management team provides essential security protection information, gains insight into potential system weaknesses and risks, and collaborates in identifying remediation and mitigation recommendations. Although not all aspects of an MBCRA lend themselves to each of the DoW RMF steps, the risk management team can use analysis results to inform DoW RMF activities. The DoW CIO guidance integrating acquisitions, cybersecurity risk management, and T&E processes (see guidance provided in the DoW CIO Library "Cybersecurity in the Adaptive

Acquisition Framework" section, https://dodcio.defense.gov/library/) captures this relationship between the DoW RMF and MBCRAs. Table G-8 provides a correlation between specific MBCRA activities and the seven-step DoW RMF process.

Table G-8. MBCRA–DoW RMF Correlation

		DoW RMF Steps						
		Prepare	Categorize	Select	Implement	Assess	Authorize	Monitor
MBCRA Activities	**Attack Path Analysis** • Identifies information processed, stored, and transmitted by the system. • Identifies potential cyberspace attack vectors into the system, paths through the system, and potential vulnerabilities along the cyberspace attack path, including the supply chain.	✓	✓	✓			✓	✓
	Cyberspace Attack Scenario Generation • Illustrates the loss of data confidentiality, integrity, and availability.	✓	✓					✓
	Risk Assessment • Quantifies the loss of data confidentiality, integrity, and availability. • Quantifies the impact and likelihood of vulnerability exploitation.	✓	✓		✓	✓	✓	✓
	Findings and Recommendations • Summarizes cyber risk assessment findings and recommendations for current and future system protection improvements.	✓						✓

G.5 MBCRAs in Intelligence

Upon completion of the assessment, the team provides informed feedback to the IC relevant to the updated cyberspace attack surface, potential vulnerabilities, system entry points and potential vectors, supply chain, and other analysis results. The IC uses this information to provide tailored products addressing areas of interest to the program manager's organization for consideration during future assessments. In addition, having this knowledge improves the IC collection and ability to inform the system development with relevant threat information. The use of focused threat information can help improve system design and operational resilience. See Appendix D: for guidance on obtaining threat assessment information.

G.6 Common MBCRA Questions and Answers

Table G-9 provides some frequent questions and answers about MBCRAs.

Table G-9. Common MBCRA Questions and Answers

Question		Answer
1	How do MBCRAs benefit the system development and program manager?	MBCRAs inform: • Cyber performance requirements • Engineering change proposals • Modeling and simulation • Test strategy development • Cyber T&E resources • Contract down-select decisions • Cyber T&E planning • Cyber T&E analysis and reporting • Recommendation prioritization • DoW RMF • Intelligence *For more information, refer to Sections G.2* MBCRAs in Systems Engineering*, G.3* MBCRAs in Cyber DT&E*, G.4* MBCRAs in Risk Management*, and G.5* MBCRAs in Intelligence*.*
2	To get the most benefit from MBCRAs, who should be involved in the process?	There are a multitude of organizations and people to consider as members for the MBCRA team. At a minimum, involve the following: • Program manager • System developer • OTA/OTO • LDTO • Participating or executing test organization • Intelligence • Operators • Maintainers • Defenders *For more information, refer to section G.1.2* Prepare: Shape Assessment*.*
3	What are the expected outputs of completed MBCRAs?	An MBCRA report is the primary method of documenting cyber risk assessments, providing stakeholders with actionable information to deliver a cyber survivable and operationally resilient system. Outputs should include: • Analysis results • Cyberspace attack scenarios • Prioritized potential vulnerabilities • Recommendations *For more information, refer to Section G.1.4* Output: Create Report/Out-Brief*.*

Question		Answer
4	Who should sign MBCRA reports?	DoW and Service policy and guidance direct MBCRAs to identify those elements and interfaces of the system, based on criticality and vulnerability analysis, needing specific attention in T&E events. However, there is no direction in terms of signatory requirements for either a report or an out-brief. Staffing the report is dependent upon stakeholder desire. The MBCRA methodology selection may also influence the signatory or routing of reports. Examples of possible signatories include the MBCRA event lead, program cyber lead, and information systems security manager. *For more information, seek guidance from the program manager or refer to the individual methodology guidebooks.*
5	How are MBCRA reports disseminated, and who has access?	The program manager owns the MBCRA reports and delivers them to senior stakeholders and all members of the MBCRA team. In some instances, the program manager may outsource the MBCRA to a third-party, but in all cases, the program manager maintains ultimate responsibility and authority. Send requests for specific MBCRA reports to the responsible program manager. The MBCRA team classifies MBCRA reports according to the specific security classification guide and usually stores all associated artifacts in the common data repository (see Section 2.2.3) commensurate with specific classification. Accessing the repository or directly receiving a copy of the report is at the discretion of the program manager. *For more information, refer to Section G.1.4* Output: Create Report/Out-Brief.
6	How does the test community use the MBCRA results?	MBCRA results directly benefit test strategy development, aid in test resource identification, and bolster test planning activities. The MBCRA results inform other documentation such as the SOW/SOO, PPP, TEMP or T&E strategy, and cybersecurity strategy. During test report generation, test teams should build upon the MBCRA cyberspace attack scenarios and observed hands-on test behaviors to provide a comprehensive analysis of anticipated system resilience in an operational environment. Following testing, the CyWG should update existing MBCRA products to incorporate validated vulnerabilities and behaviors observed during the test events. *For more information, refer to Section G.3* MBCRAs in Cyber DT&E.
7	What are the benefits of completing MBCRAs early in the life cycle?	MBCRAs are iterative activities. Teams should complete the first MBCRA early and repeat or update MBCRAs as the system development progresses and the design solidifies. Benefits of conducting MBCRAs early include: • Definition of initial set of requirements • Early understanding of potential cyber vulnerabilities • Early discussion on potential and acceptable risks • Focused threat intelligence analysis • Financial and schedule costs savings

Question		Answer
		• Early baseline, which enables rapid assessment updates to support time-sensitive decisions and activities (system functional review, system requirements review, preliminary design review, critical design review, test events) *For more information, refer to Sections G.1.2.1* Planning Activities *and G.2* MBCRAs in Systems Engineering*.*
8	How can a CyWG accomplish MBCRAs early with limited system detail or documentation?	To best accomplish MBCRAs early in the acquisition life cycle, consider subcomponents, components, subsystems, systems, and documentation from surrogate or legacy systems. Subsequent MBCRAs will build upon this data; as the design matures, so will the fidelity of the assessments. *For more information, refer to Sections G.1.1* Input: Review Artifacts *and G.1.2* Prepare: Shape Assessment*.*
9	How long do MBCRAs usually take?	MBCRA duration is dependent upon a multitude of factors and includes how long it takes to prepare for and conduct in-person event(s) and generate the final report. Assessment duration factors include: • Selected MBCRA methodology • Maturity of input artifacts • Tailoring considerations • Iteration number (baseline or update) • Resource availability (personnel, facilities) • Participation (personnel, expertise) • Time dedicated to conduct the process • Automated tool availability *For more information, refer to Section G.1.2* Prepare: Shape Assessment*.*
10	Why do MBCRAs require the generation of cyberspace attack scenarios?	MBCRAs result in the generation of cyberspace attack scenarios to aid in the design of T&E activities (see DoDI 5000.89, “Test and Evaluation”). Scenarios also codify attack path analysis results in an operational context, illustrating the potential compromise of data confidentiality, integrity, or availability, while drawing linkages to possible operational mission effects. Using this information, test teams plan and conduct scenario-based testing, aligning vulnerabilities found during hands-on testing with cyberspace attack scenarios generated during the MBCRA. Cyberspace attack scenarios illustrate the direct link between vulnerabilities and their potential impact on operational missions, highlighting the risks and consequences of successful attack scenarios, which incorporate and link system requirements to test measures and significantly improve the planning and execution of cyber T&E. *For more information, refer to Sections G.1.3* Execute: Complete In-Person Event and Analysis*, G.1.4* Output: Create Report/Out-Brief*, and G.3*MBCRAs in Cyber DT&E*.*

Question		Answer
11	Can a CyWG conduct an MBCRA without attack surface characterization?	No, this is critical input. The CyWG should complete the attack surface characterization as part of the SE activities or select an MBCRA methodology incorporating these activities. *For more information, refer to Appendix E:.*
12	Can a CyWG conduct an MBCRA without threat analysis?	No, this is a critical input. The CyWG should request threat analysis, or request results from SE activities, if available. *For more information, refer to Appendix D:.*
13	Can a CyWG conduct an MBCRA without criticality analysis?	No, this is a critical input. The CyWG should support the program protection team's criticality analysis, conduct their own criticality analysis, or select an MBCRA methodology incorporating these activities.
14	What are the typical resources required for completing MBCRAs?	Define MBCRA resources as duration, personnel, and cost. For duration considerations, refer to Question #9, "How long do MBCRAs usually take?" For personnel considerations, refer to Question #2, "To get the most benefit from MBCRAs, who should be involved in the process?" Cost is perhaps the hardest to calculate. *For more information, refer to Section G.1.2* Prepare: Shape Assessment.
15	Why should a CyWG iterate MBCRAs?	MBCRAs are vital across the life cycle of a system, providing iterative and recursive verification of the development of cyber survivable and operationally resilient systems as the system's design evolves. As a project or acquisition program matures, iterative and recursive MBCRAs inform decisions and provide updates to cyber performance requirements; engineering; transition (to warfighter, program of record); knowledge points or milestones; risk management; T&E; defensive tactics, techniques, and procedures; and operational utilization activities. *For more information, refer to Sections G.1.2* Prepare: Shape Assessment*, G.2* MBCRAs in Systems Engineering*, and G.3* MBCRAs in Cyber DT&E.
16	What resources are available to help conduct MBCRAs?	MBCRA resources vary depending upon the methodology selected. Some factors to consider include: • Methodology guidebook • Training (education, facilitator certification) • Automation (software tools) • Templates (schedules, briefings, data spreadsheets, reports) *For more information, refer to Question #17, "Where is additional help on a specific MBCRA methodology available?"*
17	Where is additional help on a specific MBCRA methodology available?	Find information on the varying organizations supporting the common MBCRA methodologies online: https://intelshare.intelink.gov/sites/resp/CTT/Shared%20Documents/0-Mission%20Based%20Cyber%20Risk%20Assessment%20Methodologies.

Appendix H: Cyber DT&E of DoW Systems Using Commercial Cloud

This appendix provides additional considerations for iterative cyber DT&E of DoW systems hosted in commercial cloud environments, supplementing Sections 3 through 7. This appendix discusses system documentation, test environments, and the diverse and complex shared cyber approaches and responsibilities. This appendix supports the development of T&E strategies tailored to DoW systems hosted in commercial cloud environments, regardless of the contracted cloud service model. This appendix does not describe how to conduct iterative cyber DT&E of cloud service provider (CSP) systems.

Appendix I: provides language for the CyWG to ensure that all commercial cloud RFPs or other requests for cloud services include iterative cyber DT&E contract language. The Requirements for the Acquisition of Digital Capabilities Guidebook provides guidance on contracts applicable to cloud-hosted IT systems contracted under DoW.

Commercial CSPs offer computing capabilities through cloud service offerings (CSOs). Cloud-hosted DoW system cyber testing should include CSOs, supporting physical and logical infrastructure (typically an abstraction layer virtualizing and logically presenting resources and services to users through APIs and API-enabled command-line or graphical interfaces) and the interfacing infrastructure for networks physically or logically connecting to the end user. The CyWG and cyber DT&E leads should refer to NIST SP 800-228 for additional API T&E considerations. This appendix uses the terms “cloud-hosted DoW system,” “system,” and “SUT” interchangeably.

Although not exhaustive, the background information in this appendix offers a framework for the general understanding required for planning and executing cyber DT&E of DoW systems hosted on commercial CSPs. This appendix does not include all the terminology used across DoW cloud efforts or the various CSPs. Reminder: This guidebook contains generalized content.

H.1 Cloud Iterative Cyber DT&E Considerations

Cybersecurity in the cloud is a shared responsibility between the CSP and the mission owner. The mission owner is the DoW Service/Component and its subcomponents using CSOs (i.e., the mission owner is the CSP’s customer).

H.1.1 Cloud Deployment Models

Cloud infrastructure deployment models host cloud services. The cloud deployment models are:

- **Private**: Provisioned for a single organization comprising multiple consumers (e.g., business units).

- **Community**: Provisioned for exclusive use by a specific community of consumers from organizations with shared concerns.
- **Public**: Provisioned for open use by the public.
- **Hybrid**: Composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology.

Early in the T&E process, the CyWG should seek a comprehensive understanding of the specific cloud service models, cloud deployment models, and the CSP and DoW tenant shared security implications. Each party should understand any additional elements in the cloud services stack and the required interfaces between the DoDIN, the cloud deployment, and potentially the rest of the Internet. The CyWG may not fully understand the specifics until selecting a CSP.

H.1.2 Test Considerations by Cloud Service Models

NIST defines three types of CSOs under the cloud service model: IaaS, PaaS, and SaaS. Figure H-1 shows the multiple stacks of cloud capability in a CSO and the typical division of responsibility for managing the capability between the CSP and the DoW program for each type of cloud service. Although these are the standard recognized services, DoW program managers may decide to design hybrid modifications of the model. Figure H-1 and the managing responsibility delineations on the stack are notional.

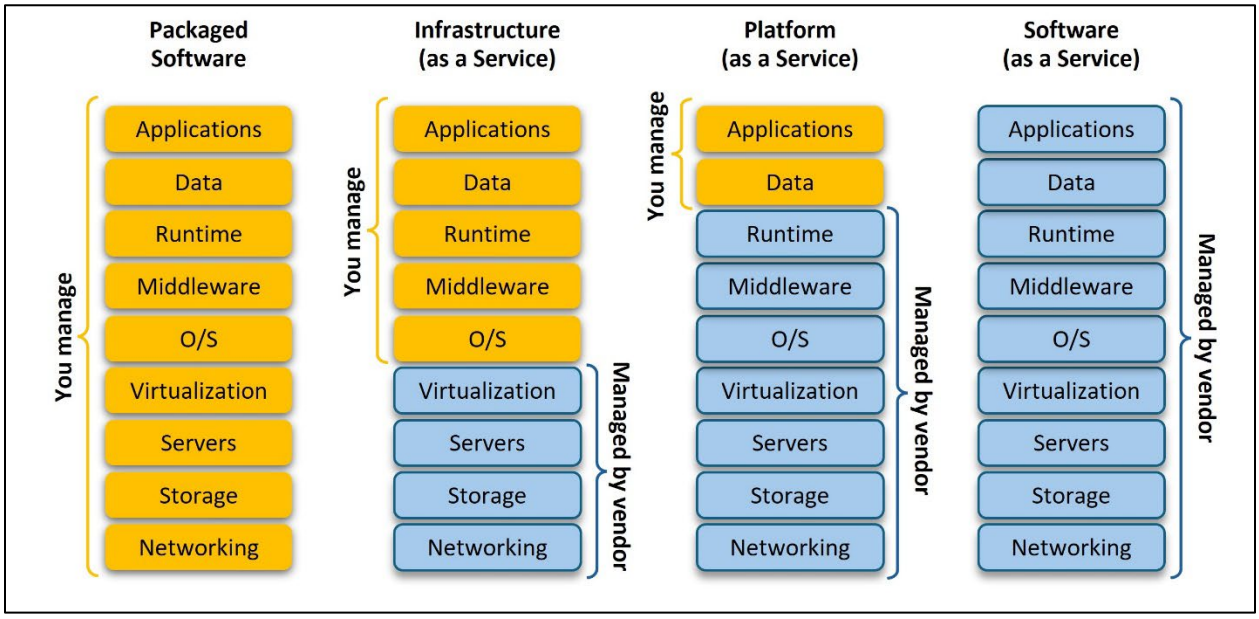


Figure H-1. Cloud Service Models

The cloud service model used by the DoW system informs the test scope. Figure H-2 illustrates how the test scope can change based on the most common cloud service models, but the test scope will depend on the details for each effort as determined during *Iterative Planning for Cyber DT&E*. Cloud research has shown that misconfiguration of the cloud service/customer-provisioned services causes most security breaches. Therefore, the scope of cyber DT&E should include evaluating the configuration of all DoW tenant-provisioned services.

As depicted in Figure H-2, regardless of the cloud service model type, the test team should consider the entire stack as part of the SUT. For the part that the DoW tenant does not "own" (and therefore has no control over the security settings), test teams should assume compromise and execute tests on the SUT accordingly.

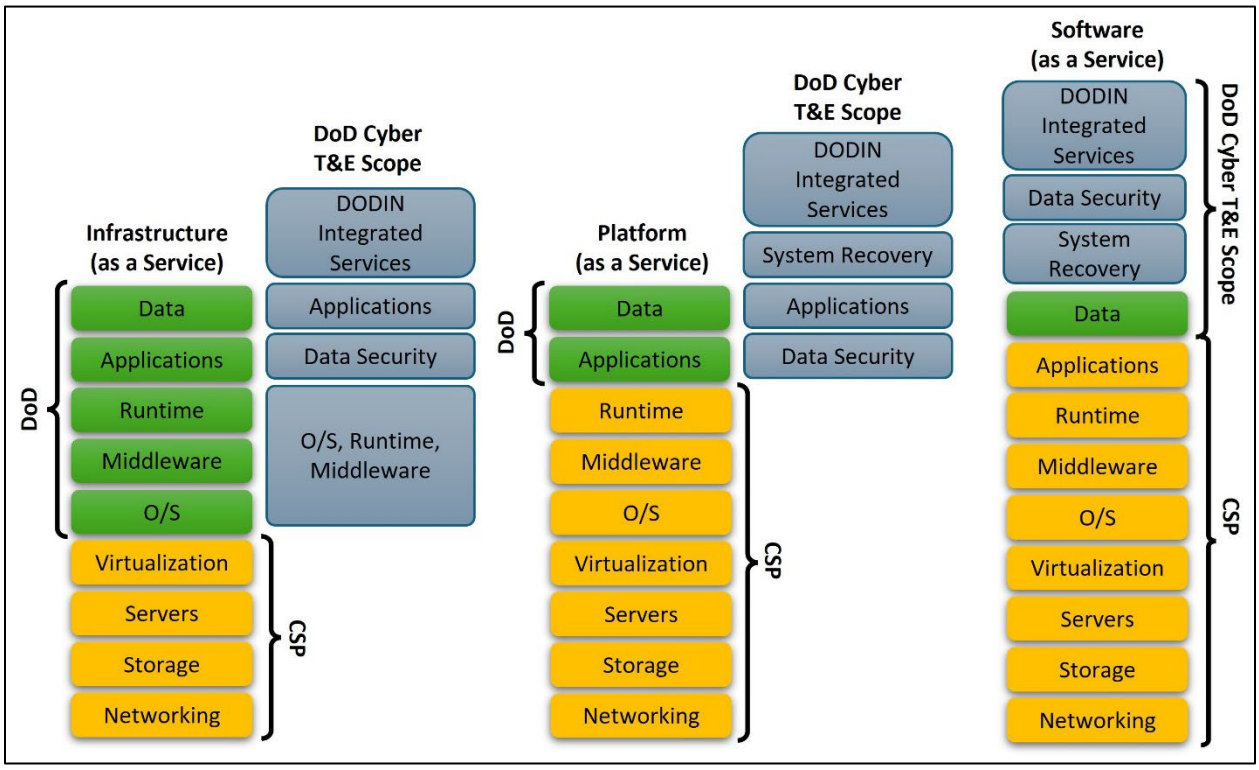


Figure H-2. Notional DoW Cyber DT&E Scope by Cloud Service Model Type

For IaaS and PaaS CSOs, the DoW system will use the CSO as a platform on which to operate a DoW application. The DoW tenant is therefore responsible for testing the DoW application and the data security provided by the DoW application and the use of the DoDIN integration points/ services.

For SaaS CSOs, test teams should, at a minimum, plan to test the CSO use of DoDIN integration points and services, data protections (access controls, use of encryption, etc.), and system recovery and availability of the provided SaaS applications. The test teams should also examine shared responsibility for security for SaaS applications.

H.1.2.1 Infrastructure as a Service

IaaS delivers compute infrastructure as a service (typically a virtualized server environment), along with raw storage and networking capability.

The DoW tenant is responsible for IaaS implementations, including providing the operating system and any necessary runtime and middleware software for DoW applications. Cyber DT&E leads should plan to test at the operating system and software/middleware and runtime layers and to test DoW tenant application and development processes, any DoDIN integration points, and DCO capabilities provided by the government and the CSP (if applicable).

H.1.2.2 Platform as a Service

PaaS CSOs allow the DoW tenant to replicate, scale, host, and secure consumer-created or acquired applications on the cloud infrastructure. The PaaS often provides a development environment to support DevSecOps software factories or application platforms such as databases, file storage, and collaborative and proprietary application processing (e.g., machine learning, big data processing, or direct API access to the features of a full SaaS application).

For PaaS, the DoW tenant is responsible for any configuration and application software installation on top of the CSO. The cyber DT&E leads should plan to test the DoW application, development environments, software factories, data security, system recovery, and any DoDIN integration points and services.

H.1.2.3 Software as a Service

SaaS CSOs are the CSP's applications running on a cloud infrastructure managed and hosted by the CSP. The DoW user will typically access the applications with a web browser, mobile application, or a lightweight client app installed on their workstation. With a SaaS, a non–DoW-developed or -owned system stores and maintains DoW data. The test scope should include the data security mechanisms implemented to protect DoW tenant data.

The test scope should include data on how long application recovery takes in the event of a CSP system failure or network outage. Cyber DT&E should focus on evaluation of the portions of the CSO where the:

- DoW tenant is responsible for configuring or customizing portions of the CSO, usually through a CSP-provided management API or web application.
- CSP and DoW tenant share security-related responsibilities.
- CSO is dependent on government services, such as DoDIN integration point interfaces between the government networks and the CSP.

H.1.3 Shared Responsibilities

The following subsections discuss most situations that a program may encounter. Contractual and legal delineations for a system prevent specifics. The CyWG should be involved early in the contracting process. See Appendix I: for additional considerations.

H.1.3.1 FedRAMP+

The Federal government authorizes a CSP to provide services to the Federal government through a program called the Federal Risk and Authorization Management Program (FedRAMP). One element of FedRAMP may include the granting of provisional authorization (PA) for a CSO on a DoW network. PA maintenance involves periodic reassessments by an accredited third-party assessment organization (3PAO) and review of the risk assessment report by the FedRAMP program management office, who has deemed it acceptable. CSPs offering CSOs to DoW should adhere to FedRAMP requirements for the relevant ILs as shown in Table H-1adapted from the DoW CIO Requirements for the Acquisition of Digital Capabilities Guidebook.

Table H-1. Cloud Information Impact Levels

Impact Level	Information Sensitivity	Location	Off-Premises Connectivity	Separation	Personnel Requirements
2	PUBLIC or non-critical mission information	U.S./U.S. outlying areas or DoW on-premises	Internet	Virtual/Logical PUBLIC COMMUNITY	National Agency Check and Inquiries
4	CUI or non-CUI Non-critical mission information Non-national security systems	U.S./U.S. outlying areas or DoW on-premises	NIPRNET via Cloud Access Point (CAP)	Virtual/Logical Limited “Public” community Strong virtual separation between tenant systems and information	U.S. Persons Single Scope Background Investigation National Agency Check with Law and Credit Non-Disclosure Agreement
5	Higher Sensitivity CUI Mission-critical information National security systems	U.S./U.S. outlying areas or DoW on-premises	NIPRNET via CAP	Virtual/Logical FEDERAL GOV. COMMUNITY Dedicated multi-tenant infrastructure physically separate from non-Federal systems Strong virtual separation between tenant systems and information	

Impact Level	Information Sensitivity	Location	Off-Premises Connectivity	Separation	Personnel Requirements
6	Classified SECRET National security systems	U.S./U.S. outlying areas or DoW on-premises CLEARED/ CLASSIFIED FACILITIES	SIPRNET DIRECT With DoW SIPRNET enclave connection approval	Virtual/Logical FEDERAL GOV. COMMUNITY Dedicated multi-tenant infrastructure physically separate from non-Federal and unclassified systems Strong virtual separation between tenant systems and information	U.S. Citizens with favorably adjudicated Single Scope Background Investigation and SECRET clearance Non-Disclosure Agreement

Additionally, the CSP should take additional steps and implement more controls to provide services to DoW organizations for data at ILs above Level 2. The additional control are necessary to satisfy the security requirements of FedRAMP+. (The "plus" signifies additional security requirements that the Defense Information Systems Agency (DISA) has built on top of what FedRAMP establishes for a risk-based approach in standardizing the adoption and use of cloud services by the Federal government. FedRAMP+ enhances the standard FedRAMP process with extra measures to meet DoW stringent security requirements. It is an evolving framework, regularly updated with new security controls and improvements to maintain exceptional cloud security standards.) The DISA AO issues PAs to CSOs meeting FedRAMP+ requirements.

The FedRAMP+ process serves as the minimum security baseline for all DoW cloud services. The CyWG should understand that FedRAMP+ and PAs are necessary but not sufficient for evaluating the shared responsibilities of CSPs and DoW tenants deploying to a commercial cloud. To maintain operational realism, the CSO should have the PAs before the start of DoW operational testing.

The CSPs, 3PAOs, and DISA develop and maintain artifacts and test results as part of the PA process.

H.1.3.2 Cyber DT&E "Of the Cloud" and "In the Cloud"

The CSP's role in providing the cloud environment, including the infrastructure and virtualization layers, gives the CSP primary responsibility for cybersecurity of the cloud. FedRAMP+/3PAO activities assess cybersecurity of the cloud for only a specific CSO and cannot replace the need for cyber DT&E.



Although the CSO PA provides inherited security assessments under the DoW RMF, the system owner is responsible for the DoW implementation of security configurations within the CSO. The system owner should define cybersecurity and cyber resilience performance for the system in the cloud and selecting and implementing additional applicable DoW RMF controls to help satisfy those requirements. The cloud service model (IaaS, PaaS, or SaaS) determines generally which areas of the CSO that the DoW tenant is responsible for securing in addition to the SUT. The cloud deployment model (private, community, public, or hybrid) determines how much of the underlying cloud infrastructure is for DoW use and is under direct DoW management. Full system testing includes testing cyber DT&E of and in the cloud, especially at the "seams" of responsibility to evaluate the security and resilience through supporting infrastructure and across interfaces down to the end user. The testing is not a reassessment of FedRAMP+ controls but of the actual defensive capabilities for the system, which includes the mission owners, users, IT operations and support (O&S) personnel, and external defenders (including managed service providers), which are the CSSPs in DoW.

H.1.3.3 Cloud Service Provider Responsibilities for Security

The CSP is responsible for maintaining the PA for the CSO and for cybersecurity "of" the cloud. The CSP's responsibilities for security depend on the type of service model used and the line between the CSP and the DoW tenant use. Although there is the potential for overlapping responsibilities, DoW may negotiate responsibilities with the CSP. The CyWG will need to fully understand where the CSP responsibilities end and where there is overlap with the mission owner or the CSSP, including what tools are available and employed by the CSP or made available to the mission owner. The contract will describe these details. At the network level, the CSP is responsible for managing and defending the interfaces between the CSO and DoDIN, involving firewalls, encryption, and automated DCO, all of which may have some government overlap as defined in the contract with the CSP. The CSP is responsible for the physical security of the servers and data storage, but the government may share the responsibility for configuring ports or user authorizations regarding these devices, depending upon the cloud service model, the CSO, and the contract. The CSP will frequently virtualize the hardware to provide the CSO. The hypervisor needed to control this virtualization is a CSP responsibility. Cybersecurity and resilience testing may include evaluating this feature.

H.1.3.4 Cloud-Hosted DoW Tenant Responsibilities for Security

The DoW tenant is responsible for developing the SLA with the CSP, which is a section of a cloud computing agreement defining the service and service levels provided and that sets performance characteristics for the CSP/CSO. Even when the CSP presets an SLA, it is important for the CyWG to understand and plan to test it.

The DoW tenant selects the cloud service model and implements the additional controls required "in" the cloud (on top of those required for the PA) to obtain an ATO for the DoW system. The DoW tenant defines CSP and CSSP responsibilities. An IaaS CSO provides the program or project with the most control, flexibility, visibility, and responsibility (see Figure H-1). The DoW tenant should create its own virtual data center above the CSP virtualization layer, including software, servers, network management, and cybersecurity monitoring and protection. SaaS provides the least amount of DoW and mission-owner control. The DoW tenant has purview only over the data entry, access interfaces, and any integration with external DoW systems. PaaS offerings fall in between, with everything but the actual application system software and data, including the operating system and database clusters, closed to DoW. The exact boundary lines and specific areas of responsibility can vary significantly among CSOs and DoW tenants.

Figure H-1 does not illustrate hidden shared responsibility or seams between the DoW tenant and the CSO, where the CSO delivers the service, but the DoW tenant is responsible for configuring it. Test teams should be able to detect misconfigurations or misapplied APIs and to work with DoW tenant leads to ensure mission-representative execution for the testing of external integration points. Programs using a commercial cloud may use an external security service provider and CSP-provided security services, which can augment and support the DoW requirement to align DoW systems with a CSSP.

H.1.3.5 Cybersecurity Service Provider Responsibilities for Security

In support of DoW DCO, DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," requires the DoW tenant to subscribe to the service of a DoW certified CSSP. Directive-type Memorandum (DTM) 24-001, "DoD Cybersecurity Activities Performed for Cloud Service Offerings," expands on DoDI 8530.01 to specify cybersecurity activities for cloud-hosted DoW systems. Refer to Table 1 in Attachment 3 of DTM-24-001 for specific details on cyber activities for each service model (IaaS, PaaS, or SaaS) by IL (e.g., IL 2, IL 4/5, or IL 6).

Program managers should identify and engage a CSSP early in the system development and include the CSSP in cyber test events whenever possible. Most of the DCO activities have T&E implications. It is important to plan and coordinate tests with the CSSP to ensure that all activities are satisfied.

H.1.3.6 Shared Responsibilities for Security

A significant difference between a traditional DoW data-center-based information system and a cloud-based system is sharing the security responsibility. DoW CSSPs, the mission owner, the

DoW tenant, and the CSP share responsibility for cybersecurity in DoW cloud-hosted systems. Each is responsible for configuring and defending different portions of the overall cloud environment.

The program manager's organization should describe clear roles and responsibilities for security in the contract and SLAs with the CSP and IT O&S personnel and in the MOA with the DoW CSSP(s). Often, the DoW mission owner is responsible for authorizing new users and roles, requesting configuration changes, and monitoring the DoW service. These areas of responsibility are different for every effort and depend on the cloud service model and the portion under the CSP's operational control. The shift in security responsibilities should be an important area of focus for DoW testing.

During the first *Iterative Planning for Cyber DT&E*, the CyWG should evaluate the coordination of cyber operations among all entities supporting the DoW system: CSSP, mission owner, DoW tenant, CSP, and IT O&S personnel. The CyWG should also understand and evaluate the technical tools, people, and processes needed to make this coordination work in support of addressing any issues identified before OT&E.

In preparation for cyber DT&E execution post–contract award, the CyWG should review MOAs with the DoW CSSP(s), IT O&S roles and responsibilities for all involved entities, and CSP SLAs. Before the DoW tenant approves these agreements, the CyWG should understand and work to resolve any identified gaps and deficiencies in these roles and responsibilities.

H.1.4 Cloud Technology and DoDIN Architecture

Figure H-3 depicts the DoDIN architecture's required integration with cloud architectures. "Boundary protections" such as Internet access points (IAPs) and cloud access points (CAPs) segregate the DoDIN from the Internet. DISA phased out the Joint Regional Security Stacks (JRSS) depicted in Figure H-3 and provides the enterprise midpoint boundary protection for the DoDIN (between the Defense Information Systems Network (DISN) and external networks). Some legacy networks use legacy midpoint protections.

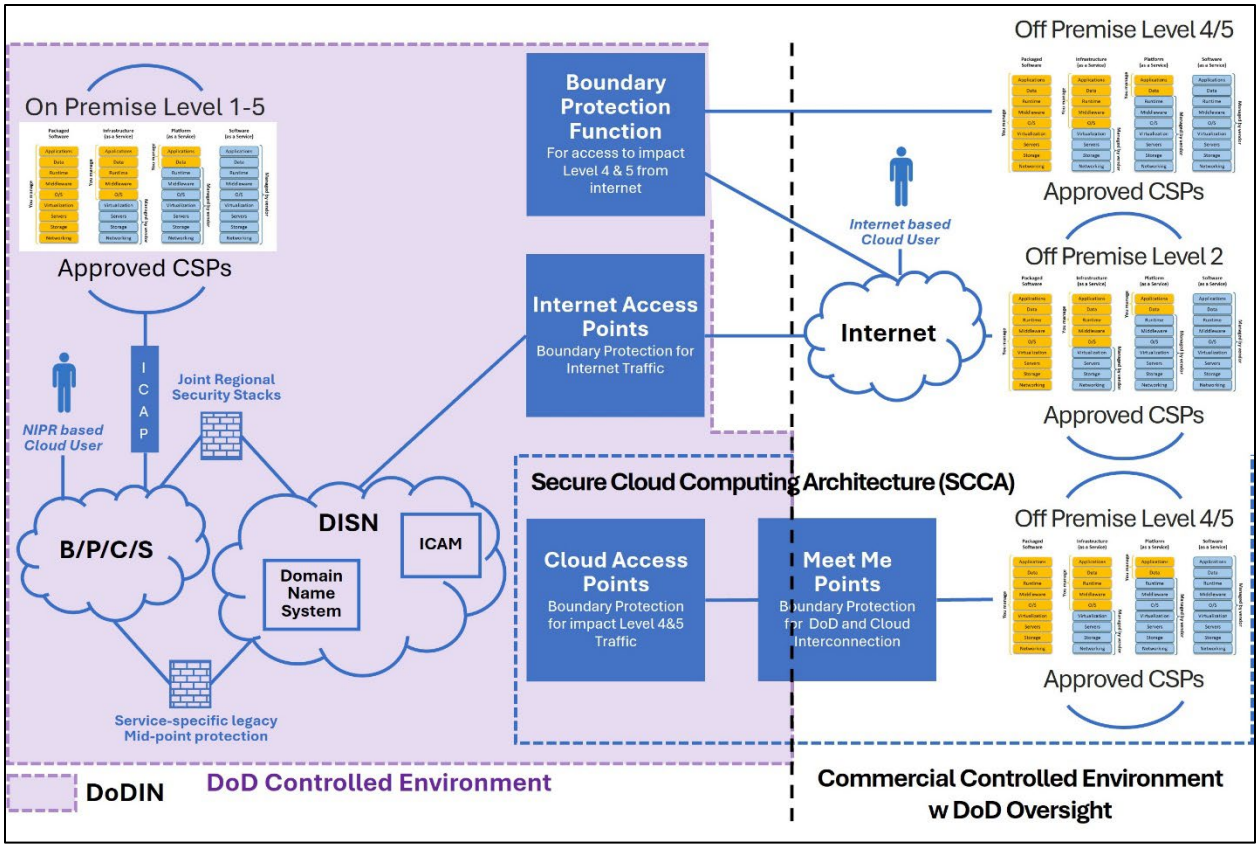


Figure H-3. Cloud Integration with the DoDIN Architecture

Figure H-3 shows how various CSOs interface with infrastructure in the DoDIN depending on their location (on-premise/off-premise) and the CSO IL. The figure shows an on-premise CSO residing on a military installation or facility base/post/camp/station (B/P/C/S) and that is within the DoDIN boundary. For an off-premise CSO, a CSP-owned facility external to a DoW installation hosts the CSO. An off-premise IL 2 CSO (sufficient when hosting only unclassified information) is directly accessible to Internet-based DoW users via the Internet and is accessible to DoW users on the DoDIN via an IAP.

As shown in Figure H-3 the DoDIN has integration points/services that CSOs should use to work in the DoDIN architecture. For example, a SaaS application that grants privileges to a user based on the user's identity would need to connect to the DoDIN Identity, Credential, and Access Management (ICAM) capability to confirm the user's identity via their CAC. DoDIN integration points/services include:

- **ICAM**. ICAM provides a single DoW authoritative source of enterprise identity supplemented with DoW Component-specific attributes as necessary.

- **Public Key Infrastructure**. This service checks for certificate expiration, verifies that a trusted certificate authority issued the certificate, and confirms the certificate's unrevoked status.
- **DNS**. DoDIN provides authoritative DNS servers on the DoDIN. CSOs should use these authoritative DNS servers.
- **CAPs**. DoDIN provides CAPs for off-premise IL 4/5 CSOs to access the DoDIN.
- **IAPs**. DoDIN provides IAPs as the boundary protection for Internet traffic.
- **JRSS**. DoDIN provided these at the cybersecurity boundary for traffic to/from individual military installations. However, DoW is phasing out the JRSS (decided in July 2021) and transitioning to a zero-trust network security architecture.
- **Zero Trust**. DoW is developing and implementing DoDIN zero-trust architecture and zero-trust network access capabilities.

DoW uses boundary protection functions (e.g., cloud-native access points (CNAPs)) allowing DoW users direct access from the Internet to IL 4/5 clouds. This method of access may be the responsibility of DoW tenants and therefore subject to cyber DT&E.

The DoW Secure Cloud Computing Architecture (SCCA) requires traffic from the CSP to traverse boundary protection (a CAP owned, configured, and defended by DISA or another DoW component) for monitoring and inspection before crossing a direct physical interconnect between the CSP and the DoDIN (a commercial Meet Me Point contracted by DISA), in lieu of connecting across the Internet. The DoW Enterprise recommends an internal CAP for on-premise CSOs, although the CSP may substitute with comparable boundary security. Each CAP should have an ATO issued by the appropriate AO. The Meet Me Point is within the scope of the CAP ATO. Therefore, Internet-based DoW users will access off-premise IL 4/5 CSOs through the DoDIN (IAP, DISN, CAP, Meet Me Point). This architecture will change in the future, however, as zero-trust architecture and zero-trust network access capabilities develop. For more information about the SCCA, refer to the DoW SCCA Functional Requirements Document.

H.1.5 Cloud Configuration Management

"Cloud configuration management" refers to the O&S of cloud resources (storage, network, software, access control, etc.), which is an important responsibility for the DoW tenant and mission owner during O&S. In-house DoW personnel or a managed service provider (e.g., a company contracted by the government to manage IT infrastructure) may perform this function.

Cloud configuration changes frequently and by various means (CSP management interface, manual adjustment, automation scripts, etc.). Cyber testing of cloud configuration is crucial, and

DoW tenants should plan and resource for this testing and coordinate testing with the cloud O&S team. The CSP management interface is a potential vector for introducing misconfigurations resulting in breaches. Additionally, because the nature of cloud is dynamic provisioning, test teams should include assessing configurations at runtime for dynamically provisioned resources.

H.1.6 Cyber DT&E Aspects of Integration Points and Services

The CyWG should include the cyber DT&E aspects of integration points and services within the scope of cyber DT&E. Test teams should be aware of the architecture and mitigation strategies implemented.

DISA is responsible for managing and defending the primary DoDIN integration points and services. As DoW Components migrate systems and capabilities to use commercial clouds, CSOs may need to interoperate with other DoW Component systems, either on an enduring basis or during the service transition period. Some DoW Components use their own midpoint protection between the DISN and DoW Component B/P/C/S networks instead of the DISA-provided midpoint protection capability known as the JRSS. In July 2021, the DoW CIO decided to phase out JRSS into a sustainment mode and transition to a new zero-trust network security architecture.

shows examples of key architectural elements (red boxes) or integration points where cyber test teams should plan to evaluate interoperability and cyber DT&E. Cyber testing should cover IAPs, CAPs, the DNS, and any zero-trust boundary protection functions. DoW published a reference design for a boundary protection capability referred to as CNAP. The DoW CNAP Reference Design describes the CNAP as a virtual IAP (or software-defined boundary). The goal of CNAP is to provide authenticated direct access from the Internet for authorized DoW users to IL 4 and IL 5 CSOs in approved commercial CSPs without having to traverse the DISN.

The DNS, IAPs/CNAPs, CAPs, and potentially other boundary control capabilities are often where security responsibilities may be poorly defined, misconfigured, or improperly understood. Accordingly, the CyWG should plan to include all integration points in the test environment to ensure a comprehensive test infrastructure.

Figure H-4 also shows examples of key operational elements (red ovals), including the CSSP and the end users, to incorporate into the test environment. The CyWG should identify, and document in appropriate artifacts, these essential architectural and operational elements during planning activities to ensure that operationally representative environments are available for the test execution activities of cyber DT&E.

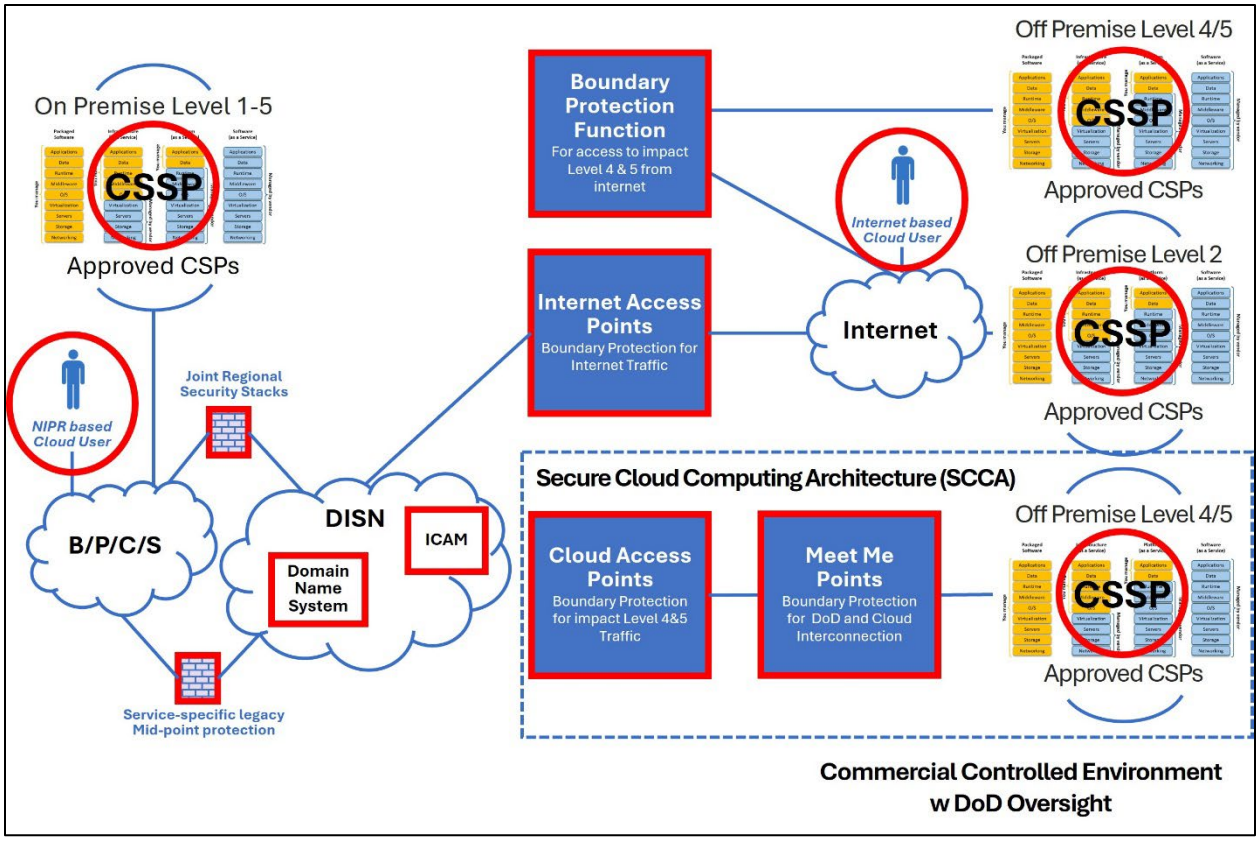


Figure H-4. Examples of Key Architectural and Operational Elements

H.2 Test Planning Considerations

The CyWG for a commercial cloud program should include cloud architects and engineers, cloud security architects, and cloud cyber testing personnel from the LDTO and the cloud cyber test system developer engaged by the LDTO. After the contract award, the CyWG should also include the CSP to help inform test planning and execution.

Early planning activities are necessary to ensure that the RFP, contract, SLA, CSSP MOAs, and other artifacts all capture the appropriate considerations for T&E.

H.2.1 Considerations During Examining and Advising on Cyber Requirements

The CyWG should examine the relevant contracts, service agreements, system designs, and preexisting test results and reports. The CyWG should accomplish the following actions as part of examining and informing cyber requirements:

- Identify and understand all interfaces to other systems, including the DoW integration points and services.

- Review:
  - The DoW tenant's contract vehicle or SLA describing cybersecurity roles and responsibilities, including test roles.
  - The cloud integration contract or task order to determine whether it covers T&E support and, if not, work with the DoW tenant to bridge any gaps and document risks.
  - The incident response plans of both the CSP and the DoW tenant to ensure adequacy and alignment.
- Identify:
  - The CSO (IaaS/PaaS/SaaS); the cloud deployment model (public, private, community, hybrid); and the IL assigned to the CSO (Level 2, 4, 5, or 6).
  - How the CSO aligns with the DoD Cloud Strategy.
- Ensure that:
  - The DoW tenant has contracted for DoW DCO support and understands what the CSP will provide to protect government data and detect data breaches.
  - The CSP provides SMEs for cyber DT&E activities.
  - The system and CSP comply with relevant security standards and regulations such as FedRAMP, NIST, and DoW-specific requirements.
- Participate in design reviews.
- Identify and document any data sovereignty or residency requirements and address them in contracts and SLAs.

H.2.2 FedRAMP Artifacts

Table H-2 lists the FedRAMP artifacts that the CyWG should leverage for cyber DT&E.

The CyWG should request artifacts produced as part of the DISA PA process documentation from the CSP or its 3PAO. The CyWG should ensure that the contract with the selected CSP articulates providing these artifacts to the government test organization.

Table H-2. FedRAMP Artifacts for Use by Cyber DT&E

Cloud Service Provider System Security Plan (SSP)	SSP Attachment 1 – Information Security Policies and Procedures SSP Attachment 2 – User Guide SSP Attachment 3 – Electronic Authentication Plan SSP Attachment 4 – Privacy Impact Assessment SSP Attachment 5 – Rules of Behavior SSP Attachment 6 – Information System Contingency Plan SSP Attachment 7 – Configuration Management Plan SSP Attachment 8 – Incident Response Plan SSP Attachment 9 – Control Implementation Summary Workbook SSP Attachment 10 – FIPS-199 Categorization SSP Attachment 11 – Separation of Duties Matrix SSP Attachment 12 – Laws and Regulations SSP Attachment 13 – Integrated Inventory Workbook
Third-Party Assessment Organization (3PAO) Security Assessment Plan (SAP)	SAP Appendix A – Security Test Case Procedures SAP Appendix B – Penetration Testing Plan and Methodology SAP Appendix C – 3PAO Supplied Deliverables
3PAO Security Assessment Report (SAR)	SAR Appendix A – Risk Exposure Table SAR Appendix B – Security Test Case Procedures SAR Appendix C – Infrastructure Scan Results SAR Appendix D – Database Scan Results SAR Appendix E – Web Application Scan Results SAR Appendix F – Assessment Results SAR Appendix G – Manual Test Results SAR Appendix H – Documentation Review Findings SAR Appendix I – Auxiliary Documents SAR Appendix J – Penetration Test Report Plan of Action and Milestones Continuous Monitoring Plan

H.2.3 Threats to Cloud-Based Systems

The CyWG should maintain currency and relevancy in understanding the threat with respect to the system. Documented cloud security threats to commercial cloud services may compromise cloud-hosted DoW systems. Threats heavily target CSPs, cloud computing services, and data. Contractors and governmental entities worldwide are targets regardless of the hosting environment, cloud, or conventional data center. The goal may be to steal or modify data; gain access to commercial and government clients' networks; or maintain persistence for the purpose of gathering intelligence, prepositioning code for later effects, and seeking financial gain through ransomware or crypto mining using the commercial cloud's powerful computing resources, thus increasing risk to DoW.

Although CSPs implement many advanced security protections, research shows that customer misconfiguration of cloud-provided security services has been the cause of most reported breaches. For example, customers have misconfigured virtual servers for public access or did not configure them to require a username and password for access. These customer configuration issues highlight the need for rigorous security validation for the DoW system. In alignment with the Cloud Security Alliance Top Threats to Cloud Computing 2024, government teat teams should develop a rigorous test strategy addressing the following cloud-based security concerns:

- Misconfiguration and inadequate change control.
- Identity and access management.
- Insecure interfaces and APIs.
- Inadequate selection/implementation of a cloud security strategy.
- Insecure third-party resources.
- Insecure software development.
- Accidental cloud disclosure.
- System vulnerabilities.
- Limited cloud visibility/observability.
- Unauthenticated resource sharing.
- Advanced persistent threats.

Program managers and system developers should be aware of these threats/security issues and develop measurable and testable cyber performance requirements aligned to the mission and to these threats enabling designed-in mitigations and defenses. The CyWG should plan to measure the effectiveness of the mitigations and defenses throughout the cyber DT&E activities.

In addition to the security concerns listed above, other emerging cloud security threats the CyWG should consider when designing cyber DT&E around cloud environments include:

- **Ransomware Attacks**. With increasing sophistication in ransomware attacks, ensure that there are robust backup and recovery processes in place.
- **Supply Chain Attacks**. Be vigilant about the security of third-party services and software integrated into the cloud environment.
- **Quantum Computing Threats**. Stay informed about the advancements in quantum computing and its potential impact on current encryption standards. Plan for future-proof encryption methods.

- **Internet of Things (IoT) and Edge Computing Vulnerabilities**. As IoT devices and edge computing become more prevalent, assess the hardening and monitoring of these endpoints.
- **Threat Intelligence Integration**. Regularly update threat intelligence to stay informed about the latest threats and tactics used by adversaries. Incorporate this intelligence into testing scenarios.

H.2.4 Test Environments for Cloud Cyber Testing

The CyWG should work in collaboration with the mission owner during *Planning* activities to ensure provisioning for operationally representative test environments to support cyber DT&E.

Mission owners deploying systems into cloud environments may be using Agile development methods or employing development, security, and operations (DevSecOps methodologies) to develop and deploy software. (See the DoD Software DT&E in DevSecOps Guidebook at https://www.cto.mil/dtea/software/ for additional considerations.) The development, test, and pre-production DevSecOps environments should support cyber testing. The CyWG should identify the need for access to these environments, tools, and products delivered in support of cyber DT&E.

If the DoW tenant can establish a test environment that fully replicates all architectural and operational aspects of the production cloud environment, including VV&A, then cyber DT&E can include a full spectrum of verification, performance, and disruptive tests against the identical, fully functional "digital twin" instantiation of the environment without scheduling constraints or fear of adverse effects to the development or production system.

Whenever possible, testing should occur on an operationally representative system. For cloud-based systems, the CyWG should consider:

- Testing the software portion of the cloud-hosted DoW system in a SIL before transitioning to the CSO.
- Using a test environment without external (live) interfaces and using replicated and representative interfaces.

Restrictions can limit testing in commercially provided implementation environments (CSOs). An alternative for testing would be to replicate the CSO in a dedicated environment at a cyber range or other DoW-owned environment to allow for destructive testing. Another is to use a DoW private cloud for development, testing, and fielding. The challenges with alternate environments arise in replicating the technical stack the commercial cloud uses due to proprietary aspects of the CSO.

The CyWG should identify test limitations and their associated risk early to allow more time to mitigate the limitations and risks.

H.2.5 Considerations During Cyber DT&E Scoping Activities

Considerations during cyber DT&E scoping activities include:

- Requesting and examining the current threat assessments. (See Appendix D:.)
- Characterizing the attack surface. Specific considerations include working with the CSO and focusing on interfaces to DoDIN integration points, interfaces, services, and DoW Component systems (if applicable). (See Appendix E:.)
- Using MBCRAs to identify mission-relevant terrain in contested cyberspace associated with critical mission functions and attack scenarios. (See Appendix G:)
    - Review preexisting and/or pre-assessed CSO environment documented threats specific to the layer of the technical architecture. The CyWG should review this documentation if available and seek to understand existing vulnerabilities and threat vectors.
    - Consider attack vectors into the CSO from other non-CSO locations in the cloud and consider the CSO capability to be an attack vector to non-CSO systems.
    - Consider attack vectors for cloud-based services including exploits targeting misconfiguration of CSO security, remote access, architecture, and authentication services by the CSO customer.
    - Examine CSO APIs used to integrate with DoDIN services that may expose the customer configuration to vulnerabilities and threats.

H.2.6 Considerations for Documenting the Cyber DT&E Strategy

The CyWG should plan for a continuum of test events and consider the following cloud-hosted specific areas of focus for documenting the cyber DT&E strategy:

- Obtain the most updated system design, including touch points into the CSO (interfaces, DoDIN integration points and services, and CSO-provided services such as data backup and storage).
- Conduct design reviews to understand the testability of the cloud-deployed application, data protections, and DoDIN integration points.
- Determine any external DoW systems with which the CSO will need to interoperate.

- Identify the CSP-provided system-level users of the SUT (administrators, help desk personnel, application administrators, etc.) and the types of cloud-based data each is authorized to view and modify.
- Determine whether the organization is deploying a new application or development project in the cloud or migrating an existing system to a CSO. The test scope may change for new application development, and migrating existing systems may involve the testing of both the legacy and new system/application. Consider whether legacy and new applications coexist.
- Review documentation on the cybersecurity roles and responsibilities of the CSSP and CSP for the DoW SUT and plan cyber DT&E activities to evaluate these capabilities.
- Examine any previous test results to determine additional testing that may be needed to ensure end-to-end assessment of the system in the cloud.
- Request, obtain, and review FedRAMP+ and PA artifacts to understand the cybersecurity capabilities that the system will inherit when using the selected CSP. The 3PAO may perform the equivalent of vulnerability test activities for a CSO as part of the assessment "of the cloud" needed to obtain a PA (at the appropriate IL) or as part of subsequent periodic continuous monitoring assessments. See Section H.2.2 for a discussion on FedRAMP+ artifacts. Additionally, the CyWG should:
  - Understand the scope of testing already performed by reviewing the 3PAO SAP.
  - Review the FeRAMP Penetration Testing Guidance available at https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance_public_comment.pdf.
  - Review available test results such as the 3PAO Security Assessment Report (SAR).
  - Identify and proceed with any additional testing required.
- Coordinate with the CSP to obtain configuration documents to assist in identifying where the system development team may have left gaps or introduced exploitable vulnerabilities into the system.
- Plan to use the cloud CSO to test the system in a representative test environment.
  - Develop a test environment strategy with the CSP.
  - For all cloud models, understand which of the CSP infrastructure layers will not be accessible to test teams and the types of tests the CSP may not allow. If necessary, develop mitigation strategies to obtain the data required for cyber DT&E.

H.3 Considerations When Preparing to Test

Building upon Section 4, cyber DT&E of cloud-hosted DoW systems should ensure that the test plan SUT description includes the portions of the DoW system for which the DoW tenant is responsible—the "in the cloud" aspects and the shared responsibilities for security. The SUTs should include all system components, interfaces, and integration points and the DCO capabilities provided by the government CSSP and the CSP. The test team should coordinate ROE with any external service provider, including the CSP, and all trusted agents identified before the start of testing. In addition to the standard tools and events used to perform cyber DT&E, the CSP can provide additional visibility into the CSO environment through native tools in the CSO as part of the service contract or through additional professional services. It may be possible to contract directly with the 3PAO who has access to test artifacts and specific CSO SMEs during testing.

The test team should ensure that the test plan covers all aspects of the system, including data storage, processing, transmission, and critical cloud test components (e.g., network setup and access policies for the cloud console). Critical components should include both the cloud infrastructure and the application layers. The test team should define clear and specific testing objectives to assess the security, performance, and resilience of the system. Objectives should include penetration testing, vulnerability scanning, configuration reviews, and incident response testing.

H.3.1 Test Objectives

Testing should collect data to support the assessments of cybersecurity and cyber resilience requirements. This section provides cloud supplemental information.

Table H-3 presents generic cloud-related test objectives cross-referenced with the most significant security risks to cloud computing as identified by the Cloud Security Alliance, an internationally recognized not-for-profit organization dedicated to promoting the use of best practices for providing security assurance within cloud computing. The table uses an "X" to pinpoint where test objectives directly intersect with potential risks, indicating areas for focused evaluation.

Table H-3 is not necessarily comprehensive, nor required, but it does identify test objectives considering the Cloud Security Alliance current security risks for cloud computing. The test objectives are applicable to all cloud service models. The CyWG should work to align these objectives to cyber performance requirements.

Table H-3. Cloud Cyber Test Objectives Aligned to Current Cloud Security Threats

		Cloud Security Threats										
		Misconfiguration/ Inadequate Change Control	Identity and Access Management	Insecure Interfaces and APIs	Inadequate Implementation of Cloud Strategy	Insecure Third-Party Resources	Insecure Software Development	Accidental Cloud Disclosure	System Vulnerabilities	Limited Cloud Visibility/ Observability	Unauthenticated Resource Sharing	Advanced Persistent Threats
Cloud Cyber Test Objectives	Verify mechanisms ensuring government data protection and control from unauthorized disclosure.	X		X	X	X	X	X	X	X	X	X
	Verify access control, identity management, and DoDIN integration.			X	X	X			X	X		X
	Verify remote administration, management of services, configurations, and consumer-defined items.	X		X	X		X			X	X	X
	Understand reuse/disposal of computer resources, storage media, and hardware, enforcing confidentiality.	X		X	X		X		X	X	X	X
	Verify dataflows, configuration protection between applications, containers, virtual devices, virtual machines, cloud service offering (CSO)/DoW infrastructure, including encryption.	X	X	X	X	X			X	X	X	X
	Verify configuration, protection, and resilience of external services (commercial or DoW cybersecurity service providers, storage, or Domain Name System).	X	X	X	X	X	X		X	X	X	X
	Verify cloud service provider (CSP) infrastructure data-at-rest encryption; leverage DoW key management.	X	X	X	X	X			X		X	X
	Verify data leak protection between applications, virtual machines, or physical infrastructure.	X	X	X	X	X	X	X	X	X	X	X

		Cloud Security Threats										
		Misconfiguration/ Inadequate Change Control	Identity and Access Management	Insecure Interfaces and APIs	Inadequate Implementation of Cloud Strategy	Insecure Third-Party Resources	Insecure Software Development	Accidental Cloud Disclosure	System Vulnerabilities	Limited Cloud Visibility/ Observability	Unauthenticated Resource Sharing	Advanced Persistent Threats
Cloud Cyber Test Objectives	Ensure that no backdoors to the CSO exist through management networks or other CSP infrastructure.	X		X	X	X	X	X	X		X	X
	Validate security monitoring (physical security and system monitoring).	X		X	X	X	X	X	X		X	X
	Verify application-level data security policy implementation on user actions and tools to monitor implementation.	X				X	X		X	X	X	X
	Verify capabilities to ensure service continuity including application and data backup and restoration, load, and capacity management.	X	X	X	X	X	X	X	X		X	X
	Verify data spillage prevention, detection, reporting, and remediation, including offboarding and sanitization processes.	X		X	X	X	X	X	X	X	X	X

The CyWG should consider the following cloud supplemental information:

- The test scope should cover the cybersecurity activities performed by both the CSSP and the CSP.
- For successful cyber DT&E, testing cannot solely rely on results from 3PAO penetration testing, which covers only the CSO ("of the cloud"). 3PAO testing does not cover the cloud-hosted DoW system ("in the cloud") nor will it focus on the DoW mission or threat. Government cyber test objectives should include stimulating mission effects and collecting system and defender prevent, mitigate, and recover actions.

- CSPs usually expose a set of APIs that customers use to manage and interact with cloud services. Organizations, via the Internet, use these APIs to provision, manage, orchestrate, and monitor their assets and users. Adversaries target these APIs and management configuration items. The CSP will need to participate in developing and enabling government testing for insider, external, and advanced persistent threat system abuse and misuse, especially for those configuration items (e.g., CSP-provided APIs) or services provided by the CSO. Cyber DT&E planning should examine the cloud-native system API protections for alignment with NIST SP 800-228. See the API cyber T&E information in the API Technical Guidance document.

H.3.2 Data Collection

Data to inform cloud cyber DT&E objectives may come from several sources: 3PAO testing, DoW tenant artifacts, and the cyber DT&E team responsible for conducting testing. Test teams should consider collecting data on the following cloud-specific focus areas:

- Both the government-controlled and CSP-provided portions of the system, including any areas where configuration, hardening, monitoring, or response responsibilities overlap.
- DoDIN integrated services, data security, and system recovery.
- Data between interfaces (e.g., during transmission between the DoDIN and cloud services).
- Data associated with identity and access management.
- Data accessibility in accordance with the CSO SLA.
- Measured resilience and recover performance defined in the contracted parameters in the event of system corruption or loss (e.g., services available 85 percent of the time during standard business hours or some other requirements).
- Data related to compliance with security standards and regulations, such as FedRAMP and NIST, to inform verifying requirements.
- Data on system performance under various load conditions to ensure that the system meets the required performance and scalability standards.
- Data from the tests of security controls (e.g., firewalls, intrusion detection or intrusion prevention system, encryption) to ensure effectiveness and proper configuration.

H.4 Data Evaluation and Reporting Considerations

Data analyses and reporting for cloud-based systems follows the guidance outlined in this guidebook. Additional cloud-based considerations include the following:

- The DoW tenant should provide raw data, analyzed data products, and test reports to the CSP to support the CSP's development of a Plan of Action and Milestones to address CSO-related vulnerabilities discovered during testing. The CyWG should track the progress of the vulnerability resolution.
- The DoW tenant should provide the data, test results, and resulting system changes to FedRAMP program management office and to the DoW PA authority, as these results may impact the FedRAMP certification and/or DoW PA of the CSO.

Appendix I: Incorporating Cyber DT&E into DoW Contracts

I.1 Background

This appendix supplements DoWM 5000.103 providing contract language considerations and other suggestions to help include cyber DT&E in DoW contracts. When crafting the cyber DT&E strategy, preceding the development of each RFP, the CyWG and test lead should identify the cyber DT&E requirements to include in a SOW, SOO, or Performance Work Statement (PWS) and in other sections of the RFP (e.g., Section C – Description/Specifications/Statement of Work). For a complete understanding of incorporating T&E into DoW acquisition contracts, refer to the WU tool, "Incorporating Test and Evaluation into DoD Acquisition Contracts." This appendix provides cyber DT&E contract considerations common across DoW Components. DoW Components should also refer to their T&E policies and guidance for specific cyber DT&E contract direction and guidance.

Include Cyber DT&E Activities in Contract Documents

It is a contracting best practice to include the government's DT&E strategy as part of the RFP to ensure that contractors understand their expected involvement and responsibilities for test planning and execution and to improve the cyber resilience capabilities of the delivered product reflected in the quality of their technical and cost proposals.

The RFP is a solicitation used in projects, acquisitions, or other transactions to communicate government requirements to offerors and prospective contractors and to solicit official legally binding proposals. The RFP Section C and resultant contract include the work statement (e.g., SOO, SOW, or PWS) that forms the basis for the contractor or system developer tasks in the S&T, prototype, pre-acquisition, or acquisition pathway.

Include Cyber DT&E Activities in Contract Documents

If contract requirements addressing cyber DT&E for verifying cyber performance requirements are not in the RFP Section C, they probably will not be in the contract. In turn, if the performance requirements are not in the contract, then the cyber DT&E will likely not happen.

If it is not in the contract, do not expect to get it!

The system developer, or contractor, plans and executes most of the testing to mature and transition the technology into the functional capabilities that the military requires. The contractor also plans and performs qualification testing of subcomponent parts and products from subcontractors composing the system delivered to the military (ICT supply chain). Therefore, the RFP and resultant contract should include provisions for the contractor cyber DT&E requirements, including system documentation; support for MBCRAs; the sharing of all test data; and visibility into the contractor's test activities, infrastructure, processes, and tools. The

insight gained from these cyber DT&E requirements can prevent redundant or unnecessary testing, but it does not remove the requirement to conduct government acceptance cyber T&E and cyber DT&E. A best practice is to pursue integrated government and contractor testing (see Section 1.6) during system development to share intelligence with the contractor and to share test tools and techniques that the government will use to optimize the find-fix-retest opportunities before the SE is no longer adaptable. Addressing cyber DT&E in the RFP ensures that the offerors are fully aware of the contractual requirements and contractually enforceable expectations to verify the cyber capabilities that enable cybersecurity and cyber resilience.

Government cyber DT&E organizational involvement during RFP development decreases the possibility of significant, disruptive, or costly changes later in system development. Program managers should tailor this appendix's cyber DT&E guidance to fit their unique situation or acquisition strategy. This guidance is based on the sequenced development process of the RFP leading to a formal contract award. Although this guidance focuses on FAR- and DFARS-based contracts, program managers should also incorporate cyber DT&E into non-FAR-based agreements (e.g., Other Transaction Authority agreements). The CyWG, in coordination with the contracting officer, should tailor the language to ensure that non-FAR-based agreements include cyber DT&E considerations appropriate for the effort.

I.2 Recommendations for DoW Requests for Proposals

The RFP describes the government's requirements (Section C); expected terms and conditions applying to the contract; information required in the offeror's proposal (Section L); and (for competitive acquisitions) the source selection criteria used to evaluate the proposal and their relative importance (Section M). The following sections of this appendix provide generic sample work statement language (Section C); instructions, conditions, notices to offerors (Section L); and evaluation factors for award (Section M). Refer to "FAR 15.204 – Contract Format" for more information on contract sections. It is important to ensure that the "right" (i.e., appropriate, understood, necessary, scoped) cyber DT&E elements are correctly and accurately included in the resultant contract. The TEMP or other T&E strategy may or may not be an RFP resultant document but requires the same cyber DT&E consideration as those generated as part of an RFP or official contract award.

I.3 Section C – General Cyber DT&E Contract Requirement Considerations

Section C of the RFP describes the work that the performers will complete and provides specifications for the goods or services that the performers will provide. This section of the appendix includes example government contract requirements typically documented in a SOO/SOW or PWS and may reference a preliminary SPS or weapon system specification. The

CyWG should ensure that the preliminary SPS or weapon system specification accurately captures all the functional cyber performance requirements to enable the required cyber DT&E.

Do not simply copy and paste these examples into RFPs and contracts.

Use this language as a guide for intelligent requirement development and contract drafting.

- The examples are meant to illustrate different approaches to ensure that contracts include appropriate cyber DT&E provisions.
- Aspects of these examples may overlap or be partially duplicative of one another.
- Carefully and thoughtfully tailor any language taken from this appendix based on artifacts, decision events, cyber DT&E activities, and phases of the project or selected acquisition pathway.

Programs or other system and technology development projects should work closely with the contracting officer to consider and tailor the example language in this appendix for their RFPs and contracts.

Another contract requirement consideration is requesting the required deliverable formats (via CDRLs and DIDs) useful for government purposes, such as automated tool cyber risk analysis. With the increased focus on SCRM, MBSE, digital twins, and other DE in general, the government should seek formats that are interoperable with digital tools. Use CDRLs and DIDs to request a standard compliant and machine-readable format for deliverables such as BOMs, SysML artifacts based on government reference architectures, and provisions for government rights. See Section I.6.

Furthermore, the CyWG should work with its servicing contracting activity to ensure the appropriate flow-down of cyber DT&E requirements from integrators or prime contractors to subcontractors throughout the entire supply chain, ICT or otherwise.

I.3.1 Contractor DoW RMF Support for Cyber DT&E



The CyWG can work with the ISSM to select and specify the test-related DoW RMF controls from Table I-1 as part of the required control set for the system under development. The SOW, SOO, or PWS should require system developer testing and delivery of the test plans and test results covered by the control set via CDRLs and DIDs. The SOW, SOO, or PWS should include provisions for the system developer, as a member of the CyWG, to ensure that testing verifies cyber survivability performance requirements during *Iterative Planning for Cyber DT&E* (see Section 3).



The CyWG specifies alignment of the controls to the mission- and safety-critical functions that the system will (or does) have with the ISSM in support of the DoW RMF Prepare Step P-4 and P-8. The CyWG aligns the test-related controls to the selected subcomponents, components, and subsystems identified by the system security working group and the CyWG after executing the criticality analysis, DoW RMF control RA-9. The CyWG should ensure that the ISSM tailors the controls and nominates them for inclusion in the contract SOW, SOO, or PWS. For each control, the SOW, SOO, or PWS should specify the required testing activity; to what mission- or safety-critical functionality the testing procedure applies; and the required deliverables in accordance with the applicable CDRLs and DIDs.

For a full description of each control, refer to NIST SP 800-53 (Revision 5 at the time of writing). When selecting a control enhancement, the ISSM should select the base control. Table I-1 provides enhanced controls for use by the developers and tailorable descriptions of the corresponding testing that the developers should perform. When there is no enhanced control, the developer should use the base control and perform the corresponding testing.

Table I-1. Test-Related NIST RMF Controls

Control/Control Enhancement	**Description**
CA-8 Penetration Testing	Conduct penetration testing on systems or system components.
CA-8(1) Independent Penetration Testing Agent or Team	Employ an independent penetration agent or penetration team to perform penetration testing on the system or system components.
CA-8(2) Red Team Exercises	Employ a red team to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement.
CP-4 Contingency Plan Testing	Test the contingency plan for the system to determine the effectiveness of the plan and the organizational readiness to execute the plan and review the contingency plan test results.
CP-4(4) Full Recovery and Reconstitution	Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.
CP-9 System Backup	Verify backups of information contained in the system with recovery time and recovery point objectives.
CP-9(1) Testing for Reliability and Integrity	Test backup information to verify media reliability and information integrity.
CP-10 System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure within the defined recovery time and recovery point objectives.
CP-10(4) Restore Within Time Period	Verify the capability to restore system components within the required restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Control/Control Enhancement	**Description**
IR-3 Incident Response Testing	Test the incident response capability for the system to determine the incident response effectiveness.
IR-4 Incident Handling	Implement and test an incident handling capability for security and privacy incidents, which includes preparation, detection and analysis, containment, eradication, and recovery.
MP-6 Media Sanitization	Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
MP-6(2) Equipment Testing	Use test sanitization equipment and procedures to ensure that the intended sanitization is being achieved.
MP-8 Media Downgrading	Verify that the system media downgrading process aligns with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information.
MP-8(2) Equipment Testing	Test downgrading equipment and procedures to verify that intended downgrading actions are being achieved.
RA-5 Vulnerability Scanning	Scan for vulnerabilities in the system and hosted applications; analyze vulnerability scan reports and results; remediate legitimate vulnerabilities.
RA-10 Threat Hunting	Conduct cyber threat hunting to search for indicators of compromise in organizational systems; and detect, track, and disrupt threats that evade existing controls.
SA-11 Developer Testing and Evaluation	Conduct periodic unit, integration, system, and regression T&E and document test results; implement a verifiable flaw remediation process to correct flaws identified during T&E.
SA-11(1) Static Code Analysis	Employ static code analysis tools to identify common flaws and document the results of the analysis.
SA-11(2) Threat Modeling and Vulnerability Analyses	Perform threat modeling and vulnerability analyses during development and during subsequent T&E of the system, component, or service.
SA-11(3) Independent Verification of Assessment Plans and Evidence	Use an independent agent to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during T&E.
SA-11(4) Manual Code Reviews	Perform a manual code review of specific code using defined procedures or techniques.
SA-11(5) Penetration Testing	Perform penetration testing.
SA-11(6) Attack Surface Reviews	Perform attack surface reviews.
SA-11(7) Verify Scope of Testing and Evaluation	Verify that the scope of T&E provides complete coverage of the required security and privacy controls.
SA-11(8) Dynamic Code Analysis	Employ dynamic code analysis tools to identify common flaws and document results of the analysis.
SA-11(9) Interactive Application Security Testing	Employ interactive application security testing tools to identify flaws and document the results.

Control/Control Enhancement	**Description**
SC-31 Covert Channel Analysis	Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert channels.
SC-31(1) Test Covert Channels for Exploitability	Test a subset of the identified covert channels to determine which channels are exploitable.
SI-3 Malicious Code Protection	Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
SI-3(6) Testing and Verification	Test malicious code protection mechanisms by introducing a known benign, non-spreading test case into the system and verify that the detection of the test case and the associated incident reporting occur.
SR-5 Acquisition Strategies, Tools, and Methods	Employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate ICT supply chain risks.
SR-5(2) Assessments Prior to Selection, Acceptance, Modification, or Update	Assess [test] the system, system component, or system service prior to selection, acceptance, modification, or update.
SR-6 Supplier Assessments and Reviews	Assess [test] and review the ICT supply chain–related risks associated with suppliers or contractors and the system, system component, or system service provided.
SR-6(1) Testing and Analysis	Employ testing of the ICT supply chain elements, processes, and actors associated with the system, system component, or system service.

I.3.2 Contractor Support to Government-Led Cyber DT&E Activities

To support government-led cyber DT&E activities, the contractor must:

- Participate in the government-led T&E WIPT or ITT and CyWGs supporting the cyber test planning, executing, evaluating, and reporting of test results.
- Supply technical or support personnel (e.g., prime contractor representatives, subcontractors, or system developers) to support the government-led T&E WIPT or ITT and CyWGs.
- Provide appropriate or available necessary data, documentation, artifacts, or other information in support of cyber DT&E activities.
- Respond to questions and provide information about the development processes, ICT supply chain, system components, logistics, and maintenance in support of cyber DT&E activities.

- Document action items, remedial activities, and other DT&E activity outcomes; record deficiencies in a risk register; and perform follow-up until satisfactory resolution in subsequent remedial or government activities.

I.3.3 Contractor Support for Mission Based Cyber Risk Assessments

To support MBCRAs, the contractor must:

- Participate in *Iterative Planning for Cyber DT&E* and *Preparing for Cyber DT&E* activities and tasks. Activities and tasks include attack surface analysis and MBCRAs. These activities and tasks will categorize potential vulnerabilities to test or analyze based on the capability of the threat and the critical functions/components.
- Supply technical personnel (contractor representatives, subcontractors, system developers) to support the MBCRA teams.
- Respond to questions and provide information about the development processes, ICT supply chain, system components, and maintenance during each step (preparation, execution, and analysis) of the MBCRA process.
- Review the cybersecurity, cyber survivability, and operational resilience requirements and the system specifications and design with government teams in preparation for the MBCRA.
- Develop the necessary data and architectural products (e.g., system attributes, internal and external interfaces, functional and system decompositions, and mission criticality analyses) to provide government teams with a comprehensive understanding of the system.
- Support the MBCRA team leads in identifying and recommending system design alternatives to minimize vulnerabilities, weaknesses, and implementation costs to improve the robustness and resilience of the system/subsystem.
- Negotiate and establish non-disclosure agreements with other contractors and the government for sharing information and technical data to fulfill the requirements of the MBCRA. The government will determine the access required by support contractors of other organizations and will provide the contractor with a list of the company names, along with a POC for those entities. The government recognizes its obligation, to the extent permitted by law, to protect the contractor and its subcontractors from competitive harm that could result from the release of proprietary data and information gathered in support of the MBCRA.

I.3.4 Contractor Support for Government Test Planning: System Documentation and Design Reviews

To support government test planning, including system documentation and design reviews, the contractor must:

- Provide system-level architectures, views, and use cases (digital artifacts, access to DE or MBSE models, digital twins, etc.) to support test planning activities and update system documentation on a recurring basis.
- Provide detailed design and architecture documentation to support test planning activities.
- Conduct a criticality analysis to accurately identify and compile a parts list for all critical components in support of test scoping activities.
- Produce a critical component list that includes the breakdown for all logic-bearing devices to the component level and all key information necessary to conduct threat assessments and testing of critical item suppliers.
- Provide a requirements decomposition from the SPS or weapon system specification to the design and product specifications reflecting criticality analysis; DoW RMF test-related controls; and the measurable and testable cybersecurity, cyber survivability, and operational resilience performance requirements.



- Provide measurable, testable, and achievable TPMs at each level of specification for cybersecurity, cyber survivability, and operational resilience decomposed performance requirements.
- Provide a contractor test strategy/plan aligned to the government TEMP or T&E strategy. Update it as necessary to maintain alignment.
- Work with government test teams to identify and eliminate potential security weaknesses, functional deficiencies, and/or vulnerabilities in support of formal and informal design reviews.
- Identify potential vulnerabilities and cyber dependencies that may impact dependent systems internal and external to the SUT (subcontractor supplier components, external software libraries, proprietary software libraries, avionics, backup power, heating, ventilation, air conditioning, commercial cloud, etc.).
- Provide previous contractor cyber test results and reports, threat assessments, and supporting test artifacts conducted for any COTS and/or NDIs to support the government's analysis for identifying system security risks. The government will

determine whether results of previous cyber testing are satisfactory to validate specific cyber DT&E requirements.

- Document action items and other DT&E activity outcomes, record deficiencies in a risk register, and follow-up until satisfactory resolution as confirmed in writing by [insert "designated contracting officer's representative (COR)," "designated technical representative," "name of the program office or some other descriptor of the government office responsible for this determination"] in subsequent remedial or government activities.

I.3.5 Contractor Testing

In conducting testing, the contractor must:

- Collaborate with government test teams to develop test cases and test scripts.
- Secure the development and test environment, processes, support personnel, and necessary tools and provide evidence of independent testing for the development environment to verify active detection of and response processes to cyberspace attacks and cyber events.
- Allow government personnel access to prime and subcontractor development environments, data, tools, analysis, and artifacts to assess and inspect the security of the development and test environments.
- Allow government personnel access to prime and subcontractor facilities to enable assessments and inspections to verify the successful implementation of security requirements not covered in the CMMC based on the criticality of the system or the sensitivity of information handled by the contractor. Ensure that the CMMC assessment, the System Security Plan (SSP), and the plans of action, including any updates, are available for review.
- Develop and test software abuse cases and network resilience abuse cases, for example, denial-of-service attacks, injection attacks, and other system misuse and abuse cases, such as pollution or taint testing.
- Develop and resource a test data collection, analysis, and management plan to equip the SUT for necessary data collection and provide support with SMEs, tools, resources, and analysis capabilities to report on test data results.
- Develop, measure, and test the system under development to verify that the system deters (prevents) cyberspace events from causing the failure of mission- or safety-critical functions or operational mission impacts.

- Develop, measure, and test the system under development to verify that the system detects anomalies or system misconfigurations caused by cyberspace events.
- Develop, measure, and test the system under development to verify that the system determines the cause of the anomaly, system misconfigurations, or design flaws.
- Develop, measure, and test the system under development to verify that the system reports facts about the cyberspace event sufficient to mitigate the anomaly or design flaw to a responsible entity, which may be a non-person entity.
- Develop, measure, and test the system under development to verify that the system enables the entity to mitigate the reported anomaly both during and after the operational mission.
- Develop, measure, and test the system under development to verify that the system recovers from the loss of mission- or safety-critical functions and maintains operational resilience in contested cyberspace throughout the life cycle.
- Verify that the system meets the functional cyber performance requirements to ensure that it is operationally resilient in contested cyberspace.
- Measure and verify specified performance requirements in representative contested cyber environments, including disrupted, disconnected, intermittent, and low bandwidth, including realistic data and communication flows. Use representative cyberspace threat TTPs against the SUT's defensive capabilities with the intent to cause mission effects.
- Measure and verify specified cyber performance requirements for system capabilities to prevent; detect; contain, mitigate, or eliminate; and recover from the loss of mission- or safety-critical functions in required mission timelines.
- Evaluate the effects of cyberspace attacks and other system faults that may lead to cascading effects (including collateral effects) in both the physical and cyberspace domains.
- Conduct cyber DT&E on subsystems, components, and subcomponents as described in the master test plan, TEMP, or T&E strategy.
- Conduct cooperative and adversarial cyber developmental testing, repeating these activities as needed to eliminate discovered vulnerabilities until delivery to the government for government acceptance cyber T&E test events.
- Conduct concurrent cyber DT&E with other functional T&E of subsystems or SoS test events such as early interoperability, KPPs, reliability, and others, as specified.

- Test to evaluate the effects of simultaneous exploitation of multiple vulnerabilities, weaknesses, system faults, and attack paths across system components or across multiple systems on a platform.
- Test for vulnerabilities that may impact dependent systems internal and external to the system under development (subcontractor supplier components, external software libraries, proprietary software libraries, avionics, backup power, heating, ventilation, air conditioning, commercial cloud, etc.).
- Provide government access to data from contractor cyber test events, including test reports from independent, third-party penetration testing of the contractor's development and test environments.
- Allow government cyber test and oversight organizations to observe contractor cyber test events.
- Verify that products are compliant with DoW STIGs and analyze exposures to known vulnerabilities within the NVD.
- Test using representative operators, maintainers, and defenders, as applicable or practicable, to assess the system and proxy defenders' ability to prevent; detect; contain, mitigate, or eliminate; and recover from the loss of mission- or safety-critical functions.
- Document action items, findings, recommendations, remedial activities, and other DT&E activity outcomes; record deficiencies in a risk register; and follow up until satisfactory resolution as confirmed in writing by [insert "designated COR," "designated technical representative," "name of the program office or some other descriptor of the government office responsible for this determination"] in subsequent remedial or program management activities.

I.3.6 Integrated Contractor–Government Cyber Testing

In addition to the suggested contract language in Sections I.3.1 through I.3.5, the following examples may support integrated contractor and government cyber testing.

The contractor must:

- Participate in integrated contractor–government cooperative and adversarial cyber DT&E test events.
- Collaborate with integrated government test personnel to facilitate the sharing of sanitized or relevant CTI information.

- Collaborate with integrated government test personnel to develop cyber DT&E test objectives, intent, resource sharing, assumptions, common test scenarios, operational mission impacts, and desired outcomes.
- Collaborate with the government to define an approach for access to, utility of, operation of, and employment of SUTs, systems supporting test, and data collection and analysis tools employed during test events.
- Collaborate with the government to develop and approve an integrated cyber test team agreement describing responsibilities.

I.3.7 Contractor Support for Government Cyber Acceptance Testing

To support government cyber acceptance testing, the contractor must:

- Provide a test system, digital twin of the system, SIL, or HWIL facility for government testing. The government may need one or all capabilities, depending on the system. A digital twin is a validated and accredited environment providing a digital replica of hardware, software, applications, processes, and connections to interfacing systems (i.e., via a cyber range) used for functional, interoperability, and cooperative and adversarial cyber developmental testing.
- Provide evidence that the contractor's digital twin is a validated and accredited test environment in accordance with DoDI 5000.61.
- Supply technical or support personnel (contractor representatives, subcontractors, system developers, test facility) to support the testing activities and government test team.
- Provide necessary data, documentation, artifacts, resource requirements, task statements, deliverables, or other information to support government test team activities.
- Respond to questions and provide information related to supporting the government acceptance testing, facilities, system, or digital twin.
- Document action items, remedial activities, and other government acceptance testing activity outcomes; record deficiencies in a risk register; and follow up until satisfactory resolution in subsequent remedial or program management activities.
- Fix, and demonstrate as fixed, all vulnerabilities identified as exploitable and mission impacting discovered during government product acceptance testing, in accordance with DoWM 5000.103. Vulnerabilities discovered during government cyber acceptance testing will result in nonacceptance and product return to the contractor for remediation.

I.3.8 Contractor Cyber DT&E Skillset and Qualifications

The RFP will describe the required core performance and supporting skillsets needed based on the size, scope, and life cycle circumstances of the project or acquisition. The core skillsets to consider for contractor personnel performing cyber DT&E are those specified in the DoW Cyber Workforce Framework for Systems Security Analyst, System Testing and Evaluation Specialist, and Vulnerability Assessment Analyst work roles. Base the required supporting skillsets on the facilities, supporting or interfacing systems, technical system support, and test infrastructure.

I.3.9 Contractor Testing for Cloud Systems

For commercial cloud contracts involving critical mission data, it is important to ensure that contract language specifically allows cyber testing using DoW-sponsored cyber test teams. The CDT or T&E lead will need support from the CSP, CSSP, and other entities to successfully execute cyber DT&E. The CyWG should ensure the RFP, the contract, and the SLA between the program manager's organization and the CSP documents the necessary requirements and testing expectations. Example PWS language includes the following:

In conducting testing for cloud systems, the contractor must:

- Deliver a CSO architecture that meets all requirements for the DoDIN, including the relevant Security Requirements Guide.
- Conduct on-demand and continuous testing [*insert minimum specification for periodicity of cycles*] to proactively discover security vulnerabilities and verify SLA metrics compliance, survivability, and operational resilience.
- Provide access to all test reports and documentation, including, but not limited to, FedRAMP+ and DISA PA-related artifacts, contractor test results of previous CSO testing (e.g. third-party penetration testing), system logs, packet capture, and other CSO information to support government cyber DT&E.
- Provide CSP technical support and SMEs (e.g., CSSP technical experts) to government-led cyber DT&E activities, including MBCRAs.
- Grant DoW physical and logical access to the CSO to conduct cyber DT&E.

For more information about contract language for commercial cloud cyber DT&E, refer to the DoW CIO Requirements for the Acquisition of Digital Capabilities Guidebook.

I.3.10 Contractor Software Testing

I.3.10.1 Software Development

In conducting software development testing for mission-critical components, the contractor must:

- Apply manual and automated software vulnerability detection methods and automated internal code-level tools (static and dynamic), application penetration and fuzz/taint/ robustness testing, and database scanning tools.
- Use third-party software assurance and ICT supply chain attack testing of development processes, the system under development, and the development environment. The contractor must flow down these testing requirements to all subcontractors for all suppliers of critical functions and associated components at all tiers.

I.3.10.2 Software Interfaces

In conducting software interface testing, the contractor must:

- Develop and provide government test teams with documentation for all software interfaces from the contractor-developed system.
- Provide test results from data validation, strong typing, and range checking for all software interfaces.

I.3.10.3 Software Tools

The contractor acknowledges that the security of its development tools directly impacts the security of the software delivered to the government. Therefore, the contractor must:

- Maintain a current, documented inventory of all software development tools (including compilers, version control systems, build tools, testing frameworks, and any associated plug-ins or extensions) used in the development of the software.
- Implement a robust vulnerability management program for all development tools, including regular scanning, remediation, and detailed records of all scans, remediation efforts, and accepted risks.
    - Configure all development tools according to DoW-approved security configuration guides (e.g., DISA STIGs) or industry best practices (e.g., Center for Internet Security Benchmarks).

I.3.10.4 Software Assurance Reporting

For software assurance reporting, the contractor must:

- Describe the software testing conducted within the system development life cycle in writing and in diagram form for illustrative purposes.
- Provide a prioritization of severity for defects and vulnerabilities.

I.3.10.5 Vulnerability Management

For vulnerability management, the contractor must coordinate with government personnel to create and implement processes that support identifying and correcting or mitigating vulnerabilities and defects during the life cycle and maintain current documentation (informed by testing) in the user manuals, Life Cycle Sustainment Plan (LCSP), and/or product support strategy.

For more information about software testing practices, refer to the DoD Software DT&E in DevSecOps Guidebook (https://www.cto.mil/dtea/software/).

I.3.10.6 DevSecOps

For DevSecOps testing, the contractor must:

- Collaborate with government development, testing, security, and operations teams early and often to encourage automation and enable consistent and repeatable testing, security, integration, delivery, and deployment practices throughout the delivery pipeline.
- Demonstrate to government test teams that the development environment is secure and free from compromise by adversaries while software development is occurring. Government test personnel will routinely audit the contractor's development environment and assigned personnel. These audits will ensure that the contractor is performing automated security testing; vetting its staff and trusted personnel; and using current, malware-free tools, libraries, and scripts.

For more information about contract language for DevSecOps testing, consult the software assurance content on JETEP (https://jetep.apps.dso.mil/).

I.3.11 Contractor Testing of Prototypes

S&T and prototype programs should generate data to inform future decisions on new concepts, technologies, components, and systems. Early cyber DT&E can reveal or enable the

development of the product's ability to meet cyber resilience requirements. In addition to overall cyber DT&E language, the following examples are specific to testing prototypes:

- The contractor acknowledges that prototypes, by their nature, may not achieve the same level of security as fully developed and operational systems. The contractor must clearly document and communicate to the government any limitations in the prototype's security posture. The government understands that the primary goal of prototype cyber DT&E is to inform future development and risk mitigation strategies, not necessarily to achieve full operational security.
- The contractor must work with the government early in the planning process to ensure that the type of cyber DT&E and the test environment is mutually supportive of the developmental environment and tools and that both provide the data and information needed to satisfy the prototype project's required security posture. This collaboration should include defining:
    - Test objectives: Clearly defined objectives for cyber DT&E, aligned with the prototype's intended functionality and potential threat vectors.
    - Test scenarios: Realistic test scenarios simulating potential attack vectors and operational conditions.
    - Acceptance criteria: Measurable criteria for evaluating the prototype's cyber resilience.
    - Data collection plan: A detailed plan for collecting and analyzing relevant data during testing.
- The contractor must allow government use of independent assessors to help plan and conduct prototype cyber evaluations and/or analyze the data generated during an experiment or demonstration. The government reserves the right to:
    - Observe all cyber DT&E activities.
    - Review and approve test plans and analyze test results.
    - Conduct independent cyber evaluations as deemed necessary.
- The contractor must deliver test results and documentation, including data rights and maintenance agreements (if applicable), to assess the product quality and cyber risk factors of the prototypes transitioning to operational use.

I.4 Section F – Deliveries or Performance

Section F specifies how and when the performer provides deliverables, such as those required in DoWM 5000.103. Section F would:

- List each deliverable specifically (CDRLs).
- Define the format, content, and level of detail required for each deliverable (DIDs).
- Establish the delivery schedule (tied to milestones in the SOW, SOO, or PWS).
- Outline government review and acceptance processes.
- Specify data rights.

Examples of suggested contract language include the following:

- The contractor must deliver all data and deliverables listed below in accordance with the deliverables schedule. All deliverables must be in a format acceptable to the government (specified in data rights and format requirements section) and must be complete, accurate, and readily usable. The contractor must maintain comprehensive records documenting the provenance and integrity of all delivered data.
- The contractor must deliver the following:
    - Attack Surface Analysis Data: Within [number] days of contract award, and updated quarterly thereafter, the contractor must deliver the most current data informing the system's attack surface analysis. These data must include, at a minimum, documentation of security strategies, plans, evaluations, and activities related to protecting and defending the DE, development, manufacturing, and test environments, processes, and tools, including software pipelines. Organize data according to Appendix E of the DoW Cyber DT&E Guidebook, Version 3.1 or current version.
    - Supply Chain Illumination Data: Within [number] days of contract award, and updated [frequency – e.g., semiannually] thereafter, the contractor must deliver data on supply chain illumination, including a detailed BOM and identification of critical suppliers. These data must include risk assessments for each identified supplier, focusing on cybersecurity vulnerabilities.
    - System Design Information: The contractor must deliver system design information, including architectural diagrams, Interface Control Documents, and dataflow diagrams, on a rolling basis as the contractor finalizes designs, with a complete deliverable within [number] days of [specify knowledge point].
    - Digital Twins, Digital Models, or Cyber Test Assets: The contractor must deliver digital twins, digital models, or cyber test assets as defined in the [SOW, SOO, PWS] and according to the schedule outlined in [Section]. Deliverables must include all necessary documentation for use and maintenance of these assets.

- Cyber Requirement Verification Traceability Matrix: Within [number] days of [system design review], the contractor must deliver a Cyber Requirement Verification Traceability Matrix in accordance with the DoW SEP Outline. The matrix must demonstrate traceability from system requirements to cybersecurity and cyber resilience performance requirements and must include supporting data demonstrating verification results.
- Test Plans: The contractor must deliver test plans aligned to Table 3 of DoWM 5000.103 during SE design and development, before the commencement of formalized testing (i.e., before integration testing). The contractor must submit test plans for government review and approval at least [number] days before implementation.
- Cyber Test Data and Reports: The contractor must deliver cyber test data and reports aligned to Table 4 of DoWM 5000.103 within [number] days of completion of each testing phase. Reports must include detailed test results, analysis of findings, and recommendations for remediation.
- Security Verification Data: The contractor must deliver security verification data, including results of vulnerability scans, penetration tests, and code reviews, within [number] days of completion of each security verification activity.
- Corrective Action Evidence: The contractor must deliver test-based evidence demonstrating that the corrective actions sufficiently remediate or mitigate mission-impacting vulnerabilities and deficiencies identified through testing and analysis, in accordance with DoDI 8531.01, "DoD Vulnerability Management." The contractor must deliver this evidence within [number] days of completion of the corrective action.

- The government reserves the right to review and approve all deliverables. The government may request clarifications or revisions to any deliverable. Acceptance of deliverables does not relieve the contractor of the responsibility for their accuracy and completeness.

I.5 Section L – Instructions to Offerors or Respondents

Section L of the RFP describes in detail the contents of each volume of the proposal. The CyWG should work with the contracting officer to insert provisions, other information, and instructions, not required elsewhere, in this section of the solicitation to guide the offerors or respondents in preparing proposals or responses to RFPs including the desired cyber DT&E information. This section will instruct prospective offerors or respondents to submit proposals or information in a specific format or in several parts to facilitate the evaluation. Section L instructions may specify

further organization of proposal or response parts, such as administrative, management, technical, past performance, certified cost, and pricing data. Example cyber DT&E–related contract language for Section L includes the following:

- Describe the plan and methodology for managing, testing, evaluating, verifying, and flowing down the cybersecurity, cyber survivability, and operational resilience requirements to subsystems and components including those provided by subcontractors/ development partners, including COTS and non-developmental components.
- Describe the plan for how the contractor will develop and execute its cyber vulnerability analysis and adversary threat analysis and how the results of these analyses can improve cyber DT&E outcomes.
- Provide a proposed approach for integrated contractor and government tests throughout development and integration of the required system capability, including roles, responsibilities, and expectations.
- Describe the proposed approach to cyber risk management, including threat analysis, system exposure to threats, operational mission impact determination, and integration of cybersecurity with SE and risk management processes.
- Describe how the contractor's processes align to the activities described in DoWM 5000.103 and the DoW Cyber DT&E Guidebook, Version 3.1.
- Describe the plan for performing cooperative and threat (adversarial) representative testing aligned to the expected threat environment of the supported capabilities.
- Describe the plan for documenting, fixing, verifying, and managing to closure exploitable and mission-impacting cyber deficiencies identified by government testing and the process for confirming that the remediation efforts did not create new vulnerabilities.
- Describe the plan for cyber DT&E to monitor and mitigate ICT supply chain risks that may impact the mission.
- Describe the plan for identifying cyber risks, vulnerabilities, and threats to important assets and functions provided by software applications.

I.6 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 communicating to offerors the criteria that the government will use to make the "best value" award decision. The contracting officer will develop the instructions included in Section L to provide guidance to the offeror concerning documentation for evaluation. Programs should draft Section L, "Instructions

to Offerors or Respondents," concurrently with Section M factors and subfactors. The alignment will ensure that the offeror provides the information needed for the government to conduct the evaluation. The source selection board will evaluate each offeror's technical, management, and cost proposals based on specific subfactors to determine whether the offeror provides a sound, compliant approach meeting the requirements of the RFP and demonstrates a thorough knowledge and understanding of those requirements and their associated risks. The Section M examples below trace back to the nine items listed in Section L items listed in Section I.5. The contracting officer might include specifics for what the government is evaluating and assessing.

Examples for Section M

The government will evaluate the proposed approach to verify cybersecurity and cyber resilience performance and the processes to recurringly verify and sustain the performance and will assess the degree to which these approaches will identify the system's threat exposure and cyber risks. The government evaluation will further focus on the following:

Factor 1: Flowing Down Requirements and Engineering. The government will evaluate this factor based on the principles of systems security engineering and SCRM as outlined in DoDI 5000.83.

- Subfactor 1.1: Evaluate the clarity and completeness of the offeror's plan for tracing and verifying cyber requirements from system-level specifications down to subsystems and components.
- Subfactor 1.2: Assess the offeror's approach to flowing down and enforcing cyber requirements with subcontractors and development partners.
- Subfactor 1.3: Evaluate the process for assessing the security posture of COTS and NDI components and mitigating identified risks.

Factor 2: Vulnerability and Threat Analysis for Improved DT&E. The government will evaluate this factor based on the rigor and comprehensiveness of the proposed analysis methodologies, aligning with the threat modeling and vulnerability analysis guidance in the DoW Cyber DT&E Guidebook Version 3.1.

- Subfactor 2.1: Evaluate the rigor and comprehensiveness of the proposed vulnerability analysis and adversary threat analysis methodologies.
- Subfactor 2.2: Assess how the offeror will integrate the results of these analyses into the cyber DT&E process to refine test scenarios and prioritize testing efforts.
- Subfactor 2.3: Evaluate the plan for incorporating current threat intelligence feeds into the vulnerability and threat analysis process.

Factor 3: Integrated Contractor and Government Testing. The government will evaluate the extent to which the offeror's proposed integrated contractor and government test approach provides visibility, data transparency, and awareness related to the cyber DT&E issues and risks of critical software, firmware and hardware components, and subsystems.

- Subfactor 3.1: Evaluate the level of detail and realism in the proposed integrated test plan, including specific test cases and expected outcomes.
- Subfactor 3.2: Assess the clarity of defined roles and responsibilities for both the contractor and the government during testing.
- Subfactor 3.3: Evaluate the proposed mechanisms for reporting test results, analyzing data, and tracking remediation efforts.

Factor 4: Cyber Threat Modeling. The government will evaluate this factor based on the offeror's ability to demonstrate a comprehensive and integrated approach to cyber threat modeling and integration with SE.

- Subfactor 4.1: Evaluate the comprehensiveness and accuracy of the proposed threat modeling process.
- Subfactor 4.2: Assess the methodology for identifying and quantifying the system's exposure to identified threats.
- Subfactor 4.3: Evaluate the integration of secure cyber resilient engineering and cyber DT&E with the broader SE and risk management processes.

Factor 5: Alignment with DoWM 5000.103 and the DoW Cyber DT&E Guidebook Version 3.1.

- Subfactor 5.1: The government will evaluate demonstrated alignment with the activities described in DoWM 5000.103 and the DoW Cyber DT&E Guidebook, Version 3.1. Provide specific examples of how the proposed approach satisfies the requirements outlined in these documents, referencing specific sections where applicable.
- Subfactor 5.2: Assess whether the offeror identifies any gaps in its approach relative to these guidance documents and proposes mitigation strategies. Offerors should proactively identify any areas where their proposed approach deviates from or falls short of the recommendations in DoWM 5000.103 and the DoW Cyber DT&E Guidebook Version 3.1. For each identified gap, the offeror should provide a clear explanation of the deviation, the rationale behind it, and a detailed mitigation strategy to address the potential risks associated with the deviation. Mitigation strategies should be SMART.

Factor 6: Cooperative and Adversarial Testing. The government will evaluate this factor based on the extent to which the proposed testing approach supports the development and execution of a robust cyber T&E strategy, as described in the DoW Cyber DT&E Guidebook Version 3.1.

- Subfactor 6.1: Evaluate the realism and relevance of the proposed threat environment for cooperative and adversarial testing.
- Subfactor 6.2: Assess the methodology for conducting cooperative and adversarial testing, including the use of red teams and penetration testing techniques.
- Subfactor 6.3: Assess the approach to verifying the effectiveness of the defense-in-depth strategy in supporting the delivery of defense-in-depth capabilities (i.e., DCO).

Factor 7: Deficiency Remediation and Verification. The government will evaluate the contractor's process to document, fix and verify fixed exploitable and mission-impacting cyber deficiencies identified by government testing and how the contractor will confirm that remediation does not introduce new known vulnerabilities.

- Subfactor 7.1: Evaluate the process for performing root cause analysis of identified cyber deficiencies.
- Subfactor 7.2: Assess the comprehensiveness of the regression testing plan to ensure that remediation does not introduce new vulnerabilities.

Factor 8: ICT SCRM Mitigation (Cyber DT&E Focus). The government will evaluate the contractor's process to monitor and perform cyber DT&E of its development environment to mitigate ICT supply chain risks that may impact the operational mission.

- Subfactor 8.1: Evaluate the plan for continuous monitoring for vulnerabilities in ICT supply chain components.
- Subfactor 8.2: Assess the proposed strategies for mitigating identified ICT supply chain risks.

Factor 9: Software Application Cyber Risk Identification. The government will evaluate the offeror's ability to identify and assess cyber risks specifically associated with software applications, focusing on comprehensive asset identification and robust vulnerability management practices.

- Subfactor 9.1: Asset Identification: Evaluate the process for identifying critical assets and functions provided by software applications.
- Subfactor 9.2: Vulnerability Scanning and Analysis: Assess the methodology for performing vulnerability scanning and analysis of software applications.

I.7 Cyber DT&E Suggested Deliverables

Table I-2 is an example of known CDRLs and the associated DID related to cyber DT&E for the CyWG to consider including in the contract. CDRLs provide the data the contractor should deliver and include the descriptions of the format, content, and usage of the data. The CyWG should work with the contracting officer to tailor CDRLs to project requirements or the selected acquisition pathway to ensure delivery of the correct information/ data by the contractor and to avoid excessive documentation. Other parts of the contract may require engineering-related plans and documentation that the government test personnel will need to support key analysis and test planning activities necessary to achieve cyber DT&E objectives. During RFP development, the engineering team and test team should collaborate to identify applicable deliverable documents, avoid duplication, and streamline the format of the required documents as appropriate, including consideration if government or contractor tools enable automatic artifact generation.

Additional Information

For more information on CDRLs:
https://www.dau.edu/blogs/product-support-contract-data-requirements-list-cdrl

For more information about CDRLs and DIDs:
https://www.dau.edu/acquipedia/pages/

See the ASSIST database for details of the referenced DIDs listed in Table I-2:
https://quicksearch.dla.mil/qsSearch.aspx

Table I-2. Test-Related Contract Deliverables

CDRL	CDRL Title and Description	DID (Reference: ASSIST)
CTE001	Cybersecurity Test Plan – detailed test plans for contractor test events	DI-MGMT-82140A
CTE002	Cybersecurity Test Procedures – planned test methodologies, including code evaluations, functional testing, penetration testing, fuzz testing, vulnerability scans, third-party assessment, and off-nominal test cases	DI-MGMT-82141A
CTE003	Cybersecurity Test Report – T&E report for each test event	DI-MGMT-82142A
CTE004	Vulnerability Assessment Report – contractor-identified vulnerabilities and corrective action/mitigation plans	DI-MGMT-82135A
CTE005	Vulnerability Scan Compliance Report	DI-MGMT-81842
CTE006	Software Test Plan	DI-IPSC-81438A
CTE007	Software Test Report	DI-IPSC-81440A
CTE008	Test Plans/Test Procedures	DI-SESS-81704
CTE009	Survivability Analysis Report	DI-MISC-80564B

CDRL	CDRL Title and Description	DID (Reference: ASSIST)
CTE010	Software Assurance Evaluation Report	DI-IPSC-82249A
CTE011	Software Attack Surface Analysis Report	DI-IPSC-82250A
CTE012	DoD Risk Management Framework (RMF) Package Deliverables	DI-MGMT-82001A
CTE013	Contractor's System Security Plan and Associated Plans of Action to Implement NIST SP 800-171 on a Contractor's Internal Unclassified Information System	DI-MGMT-82247
CTE014	Bill of Materials (BOM) for Logistics and Supply Chain Risk Management	DI-PSSS-81656B
CTE015	Supply Chain Risk Management Plan	DI-MGMT-82256A
CTE016	Hardware Development Plan	DI-MISC-80508B
CTE017	Counterfeit Prevention Plan	DI-MISC-81832
CTE018	Anti-Tamper Plan	DI-MISC-80508B
CTE019	Contractor's Record of the Tier 1 Level Suppliers Receiving/ Developing Covered Defense Information	DI-SCRE-82258

I.7 Contract Incentives

Incentives as part of the RFP development process can encourage high-quality performance to achieve cyber and operational resilience goals. Cyber incentive provisions can also improve a system's risk posture, especially in S&T projects, pre-acquisition projects, and urgent capability and middle tier acquisitions (see Section 8), which may use proven or mature technology and where there may be little if any visibility into prior cyber testing. To be most effective, the contracting officer should apply incentives to performance targets that the contractor expects to accomplish rather than to the minimum cyber DT&E requirements. DoWM 5000.103 requires government acceptance cyber T&E. Consider contractual incentives to reward the contractor if the government does not identify any critical deficiencies during government cyber acceptance testing.

Another consideration for incentives is whether the government has incorporated a contractor and government integrated test approach into the test program. Frequent collaboration may reduce the need for incentives if the government can embed its test teams, and they can contribute and have access to the contractor's SE and testing data and processes during system development. *Preparing for Cyber DT&E* focuses on the system or technology and will also inform whether incentives are necessary to mitigate known and potentially mission-impacting vulnerabilities.

By using this appendix, program managers can ensure a robust contractor cyber DT&E approach that uses disclosures to find and quickly remediate problems. Example vulnerability data shared by the contractor could be:

Incentivize the Sharing of Discovered Vulnerabilities

To encourage early (and therefore more cost-effective) mitigation of cyber vulnerabilities by the contractor, program managers can consider award fee incentives focused on proactive mitigation and vulnerability discovery and remediation verification with government cyber test teams. Talk to the servicing contracting officer if award fee incentives may be appropriate.

- Number of vulnerabilities discovered in each critical component.
- Severity (Service-specific).
- Type: OWASP Top 10/CWE Top 25.
- Discovery: How the contractor identified the vulnerabilities.
- Fixed: How many vulnerabilities the contractor fixed.
- Time to repair related to priority to repair.
- Measurable impact that the vulnerability remediation has on cyber survivability requirements.
- Cost, schedule, or performance improvements due to remediated vulnerability.

For more information on incentives and award fee contracts, see the WU tool, "Incorporating Test and Evaluation into DoD Acquisition Contracts."

Appendix J: Cyber DT Infrastructure and Environment Planning

J.1 Purpose

This appendix assists the CyWG in planning cybersecurity test infrastructure for the entire system life cycle, from development through sustainment. Test objectives and data inform infrastructure planning by identifying necessary capabilities. Early cyber DT&E analyses and MBCRAs clarify what to test, including suspected vulnerabilities, critical system data, components, and functions essential for mission success, and operational concepts clarify the required testing conditions. Just as the CyWG will iteratively review and update the requirements for testing, the CyWG will also iteratively review the requirements and plans for the test infrastructure. This review is necessary to satisfy the cyber DT&E parameters in DoWM 5000.103, including crafting testing environments to characterize the attack surface using all available system architectures and other artifacts to identify all forms of communication, network connectivity, software, hardware, ICT supply chain, and human interaction. This process is also consistent with DoDI 8510.01, "Risk Management Framework for DoD Systems." Without duplicating resource demand, all cyber stakeholders should be proactively communicating test results, enabling process integration and remediation prioritization for warfighter benefit.

J.2 Infrastructure Planning for Cyber DT&E Across the Life Cycle

Cyber DT&E, using both system developer and government test facilities, begins with systems development and continues through fielding and sustainment. Each stage of the system's life cycle needs test infrastructure and environments. Testing starts with verifying the smallest components of the SUT in development environments and progressing to integrated test (see Section 1.6) with the complete SUT and system interfaces using a production-representative system with trained, typical users, maintainers, and defenders performing operational missions in an operationally representative environment.

J.3 Infrastructure Planning for Cyber DT&E

Several factors inform planning for test infrastructure including test objectives, MBCRAs, previous testing, and other *Iterative Planning for Cyber DT&E* activities. The CyWG should include this infrastructure in the TEMP or T&E strategy. Table J-1 lists topics that the CyWG should consider when planning for the cyber test infrastructure.

Table J-1. Cyber DT&E Test Infrastructure Planning Considerations

Topic	Considerations
SUT technology maturity and software licensing	Use mature hardware and software specifications to plan the test environment. Base planning on the most mature system configuration needed to support the test objectives. Identify any software licenses to support the test environment.
System security classification	Identify all security classifications for the SUT. Review the SUT configuration for each classification level to identify similarities and differences affecting the test infrastructure.
Data collection method and format	Identify and correlate data collection methods and formats with needed data and measures. Consider all data collection methods, including automated instrumentation, observers, system logs, video, and audio. Identify available data collection tools, including modifications. Identify data collection tools that need developing.
Personnel requirements to support the test infrastructure	Identify the types of qualified range personnel, vulnerability test teams, and red teams (and performance and defense test teams for cyber operational testing).
Network availability and bandwidth, including traffic simulation tools	Review the requirements to create representative network traffic volumes and dataflows. Confirm the ability of test infrastructure to provide the expected traffic levels and content during normal and stressed operations. Confirm the need and ability of test infrastructure to simulate communications throughput and bandwidth such as local area networks, satellite communications, and tactical communications.
Availability of representative cyber terrain and attack surface	Identify whether the test infrastructure can represent the cyber terrain components and attack surface elements within the SUT.
Test resources	Review the complete list of resources such as test ranges, tools, and equipment including needed hardware, software, and models and simulations. Identify the verification, validation, and accreditation status for ranges and for modeling and simulation.
System restoration	Define the responsibilities and procedures for restoring systems and infrastructure to their pre-test state. Include processes for system and cyber restoration, ensuring the removal of all cyber threats introduced during testing from the test environment and infrastructure. Test and evaluate the effectiveness of restoration procedures, including validation of the target's cyber aspects and the processes and media used for restoration.

J.3.1 Initial Infrastructure Considerations

Initial analysis of requirements and system design typically does not consider test infrastructure. Requirements examination should inform funding profiles and ensure that the RFP includes provisions for cyber test facilities, tools, and metrics, considering anticipated classification levels and security. The CyWG should contribute cyber testing requirements to the RFP, which should clearly state the test articles, virtual images, virtual SILs or other test labs, ranges, and other models needed to support system developer and government cyber testing in either system developer or government facilities such as a government cyber range or SIL. As appropriate, the RFP should require system developers to expose systems and networks to realistic cyber threat testing in a closed test facility by independent cyber professionals using the latest tools, techniques, and procedures to evaluate the system design. The RFP also might require the system developer test environment to include emulated or actual connections to external systems/labs and representative dataflows.

The RFP should discuss provisions for both government access to and use of system developer test infrastructure, and system developer access and use of government infrastructure. For example, the government may want to consider resourcing the system developer to develop cyber T&E infrastructure for government use, such as a SIL. Alternatively, the government may arrange for the system developer to use government cyber ranges.

The CyWG should consider requesting virtual, restorable images and test articles to support early government cybersecurity and cyber resilience testing in lab environments. Virtual, restorable images can range from a reusable instantiation of the system all the way to a virtualized SIL. These images support replay of test activities, destructive threat testing and rapid reconstitution of the test environment, and exercise restoration capabilities, and they can improve fidelity to represent realistic mission operations.

Government test teams should understand the system developer test infrastructure to assess the amount of visibility needed into proposed test activities. The teams should identify when to require data collection and when data transfer will benefit government test activities to reduce redundancies or unnecessary testing.

J.3.2 MBCRA Infrastructure Considerations

MBCRA events (see Appendix G: for more information) are essential for scoping considerations and to clarify the components and testing tools needed for the cyber test infrastructure and environment. Early identification of unique tool requirements during these events may support tool development by the DoW Component or enterprise investment, such as leveraging the TRMC Central T&E Investment Program's cyber quick-reaction test capability. The CyWG should use MBCRAs to inform the planning of test infrastructure, ensuring effective support for

testing mission- and safety-critical functions. Furthermore, an MBCRA analysis informs the following cyber infrastructure and environment components:

- **Cyber threat**: Portraying a cyber threat requires infrastructure to support emulating adversaries with different levels of physical and logical access using representative tools and TTPs.
- **Cyber terrain**: Test infrastructure should contain either live or simulated components of the operational environment including items inherent to and provided by the SUT and those within which the SUT operates such as networks, cyber defenses, and interfacing dataflows.
- **Attack surface**. Test infrastructure encompasses relevant aspects of the complete attack surface.
- **Defenders**. Test infrastructure should either support live defenders or emulated defenders, depending on the scope of the test event and interfacing systems.
- **Missions**. Test infrastructure should enable the SUT to operate in the context of users completing operational missions.

J.3.3 Cyber DT&E Infrastructure Considerations

Cyber DT&E includes testing of the SUT in an environment ranging from a virtual SIL or another closed environment to the SUT deployed in the operational environment. Subcomponent, component, subsystem, system, and integrated system or SoS cyber DT&E can take place in system developer or government test facilities. Infrastructure planning for cyber DT&E should consider:

- System developer cyber testing and government acceptance testing of the cyber posture and cyber resilience capabilities of subcomponents and components.
- Government SILs for testing integration of the subcomponents and components into subsystems and into the system itself. If the system developer has not tested to the component level, then the government test infrastructure should also support component- and subsystem-level testing using an environment closely mirroring the system developer's development environment. The CyWG should plan the testing of all components before system integration testing and deployment into an operationally representative environment.
- Cooperative tests that include cyber defenders and their infrastructure components such as sensors for attack detection and log collection tools, especially if the cooperative test includes penetration testing.

- The ability to use and availability (e.g., scheduling, contractual limits) of models, simulations, and digital twins for cyber tests.

J.3.3.1 Development-Test Labs and System Integration Labs

Development-test labs and SILs provide environments for software testing, hardware component testing, subsystem integration, and system integration. A SIL may include simulators or emulators when needed to exercise system components early in the system life cycle. SILs are risk-reduction facilities supporting the development, integration, and testing of software and hardware. Additional software assurance testing resources and capabilities are available through JETEP (https://jetep.apps.dso.mil).

A SIL should allow the testing of all data connections and flows using simulators. The SIL test environment should include facilities to test system restoration by testing at the component and system levels during system development. These environments can support functional intra-operability (internal interoperability of integrated components) T&E and cyber DT&E.

J.3.3.2 Adversarial Infrastructure Considerations

Adversarial testing examines the mission effects from a system's cyber posture and cyber resilience in a mission context in an operationally representative environment. The CyWG should plan to replicate the system and SoS in the representative test infrastructure, including the network environment with network traffic, system interfaces, dataflows maintenance interfaces, remote access configurations, and at least a proxy CSSP.

The CyWG should consider using a closed-loop cyber range to conduct adversarial tests. Cyber ranges and HWIL facilities may provide representative environments for demonstrating cyber effects while minimizing the risks to operators, defenders, and operational networks. Other potential candidate test infrastructures include SILs, hardware integration labs, digital twin facilities, and virtualization labs.

The test environment needs the flexibility to alter, compromise, and corrupt the SUT and then recover it to the original operating conditions to allow multiple test runs. This flexibility supports the test team's ability to represent and evaluate the diversity of tactics that a cyber adversary might use. Adversarial test planning should include time for infrastructure setup and pre-test verification and time to sanitize the environment and start over, not just the test event timeframe. Test teams should also plan adequate time in the test environment to explore SUT configuration settings to optimize cyber defenses.

J.3.3.3 Building Representative Contested Cyber Environments

Composing a live, virtual, and constructive representative cyber battlefield environment requires seamless interoperability among the involved DoW labs, facilities, and capabilities. Contested cyber environments, however, were not always a consideration during the design of many of these capabilities. The labs may require additional planning and resources to support cyber DT&E.

For individual weapons or platform systems, it may be necessary to build the entire SUT in a mission-representative environment. The following core DoW infrastructure is available to integrate or connect with additional DoW and non-DoW capabilities to create the required environments:

- Joint Mission Environment Test Capability (JMETC) Multiple Independent Levels of Security (MILS) Network (JMN). The JMN connects facilities to support testing, training, and experimentation. The test team may execute events locally using secure test rooms or remotely via the Joint Information Operations Range (JIOR) and the JMN. In general, the JIOR provides connectivity for sites used primarily for training or operations, whereas the JMN provides connectivity for sites used for acquisition research, development, T&E.
- Regional Service Delivery Point (RSDP). RSDPs provide distributed computing and storage platforms to enable a flexible and adaptable infrastructure and to support a contested cyber environment. RSDPs also provide a closed-loop community cloud computing capability.

J.4 Cyber T&E Infrastructure Planning in the TEMP or T&E Strategy

Appendix K: provides a detailed discussion of the necessary elements for the cyber DT&E strategy. The following list provides key inputs for the integration of infrastructure planning in the cyber DT&E strategy:

- Test environments planned for cyber testing, including system developer and government facilities.
- How the test environment will incorporate the system interfaces.
- The emulated, live, virtual, or constructive aspects.
- Test infrastructure and reference facilities such as development-test labs, system integration facilities, and cyber ranges.
- Data collection environment and the plans to collect required data.

- The resources already available and the resources still needed, including:
  - Cyber ranges or specific tools.
  - Resources required to use the test environment described, including funding and responsible organizations.
  - Resources for the test environment in terms of tools, data collection, and staff.
  - Resources allocated to the SUT and test articles and whether the article is reusable or not (HWIL, SIL, virtual systems, etc.).
  - Hardware and software requirements.
  - Specific systems/networks planned to connect.
  - System/network architecture.
  - External connectivity needed for remote cyber range support.
  - Instrumentation requirements.
  - Traffic generation requirements specific to the mission environment.

Appendix K: Cyber DT&E Strategy Considerations

K.1 General Guidance

As discussed in Section 3.5, the TEMP or T&E strategy should describe a strategy for cyber DT&E that uses relevant data from all sources and includes a summary of system developer testing activities, integrated government testing (see Section 1.6), and concurrent cyber and non-cyber testing (see Section 1.7). Data sources may include security controls assessments; MBCRAs; subcomponent-, component-, and subsystem-level tests; and SoS tests. The TEMP or T&E strategy should explain the alignment with other acquisition functional efforts, including:

- Program protection (e.g., ICT SCRM, software assurance, criticality analysis, and trusted systems and networks analysis).
- DoW RMF (e.g., SAP, configuration management).
- Interoperability (e.g., Information Support Plan (ISP)).
- Sustainment (e.g., LCSP).

Additionally, the TEMP or T&E strategy should provide details on:

- The cyber DT&E strategy to align testing requirements associated with not only system cybersecurity standards (STIGs, scanning) but also cyber resilience within a mission context.
- The cooperative and adversarial testing events on interfaces, subcomponents, components, subsystems, and systems through an iterative approach that includes mitigations informed by the mission- or safety-critical functions.
- How data collection from cyber developmental testing informs deficiency reporting and describes the process for managing cyber deficiencies, including a clear timeline that supports mitigating exploitable system vulnerabilities impacting operational resilience.
- Recording and tracking how system deficiencies from cyber effects and fixes address cyber safety, cybersecurity, and cyber resilience performance requirements in support of assigned missions.
- The testing of defensive capabilities (monitoring, logging, responses), recoverability, and sustainability.

K.2 Cyber DT&E Information for the Body of the T&E Strategy

The CyWG actions detailed in the following subsections guide them in helping the CDT or T&E lead document the appropriate cyber DT&E strategy–relevant considerations in the TEMP or T&E strategy.

K.2.1 System Description in the T&E Strategy

Briefly describe the SUT, the system configuration, and the unique features supporting cybersecurity and cyber resilience. Identify whether the system has specialized components such as cross-domain solutions, industrial control systems, non-Internet data transfers, and data transfer via alternate media such as RF and data links (see the CUI Appendix L). Document the attack surface. Specialized components should drive specialized cyber DT requirements.

K.2.2 System Threat Assessment in the T&E Strategy

Describe the cyber portion of the complete threat environment in which the system will operate (e.g., the system will operate in contested cyberspace against a variety of cyber threat actors). See Appendix D: for information on how to obtain cyber threat assessments for the DoW IC. In the TEMP or T&E strategy, reference the applicable threat documents (VOLT Report, relevant threat libraries), if available, including the most recent DIA Computer Network Operations Capstone Threat Assessment and the DoW Component-validated threat documents for the system. Outline the expected types of cyber threat actors who may intend to target the system or its mission(s) (e.g., a full range of cyber adversaries with nascent, limited, moderate, and advanced capabilities) and the threat actor's capabilities (e.g., exfiltrate, infiltrate, or corrupt data; disrupt system operations; physically destroy equipment). Identify where to find additional cyber threat information for the SUT.

K.2.3 Systems Engineering Requirements in the T&E Strategy

The CyWG should ensure that the strategy includes a high-level discussion of how SE integrated cybersecurity and cyber resilience performance into the system architecture and design, including the use of any applicable results from previous MBCRA findings. The strategy may explain whether systems engineers used and applied DoW RMF overlays and technical security controls (or if the system has inherited protections) and any other DoW RMF tailoring activities. The CyWG should discuss how activities such as iterative MBCRAs and cyber tests will inform design changes and risk mitigation activities. The SE requirements section of the TEMP or T&E strategy should also align with the respective cyber test discussions in subsection K.2.8.



K.2.3.1 Program Protection Requirements in the T&E Strategy

The cyber DT&E strategy may require efforts to verify the requirements in the PPP and PPIP. Consider the items in Table K-1 when discussing program protection requirements in the TEMP or T&E strategy.

Table K-1. Program Protection Requirements

Requirement	Description
C-SCRM	Describe the system developer's and program manager organization's plans for managing cyber supply chain risk management.
Critical Components	Discuss the efforts and ability to illuminate tiers of the ICT supply chain for critical components identified in the Program Protection Plan/Program Protection Implementation Plan.
CMMC	Examine the Cybersecurity Maturity Model Certification status for the critical components and describe managed and unknown risks.
Attack Surface	Describe the system developer's plan to evaluate the attack surface exposure from the developer's environment, tools, and processes.
Risks	Describe managed and unknown risks.

K.2.4 Special Test or Certification Requirements in the T&E Strategy

Identify any unique system characteristics or support concepts that will generate special cyber test, analysis, and evaluation requirements and any anticipated test, analysis, and evaluation activities meeting those requirements. Identify and describe all required certifications informed by cyber test and analysis (if applicable). Discuss the integration of cyber DT&E activities with the DoW RMF process as outlined in DoWM 5000.103. Use the special test or certification requirements section for cyber test activities requiring special tools, environments, and personnel.



K.2.5 Previous Testing Documented in the T&E Strategy

Highlight the cyber assessment and testing history of the system by listing pertinent past assessments and test events that will inform the cyber test strategy and future test activities. Provide the location for accessing the past test data and reports and the accessibility requirements for non-program personnel (e.g., test organizations, OSD oversight organizations). Include assessments and tests performed during the Analysis of Alternatives phase and any previous cyber analysis or testing performed on expected components (including the testing accomplished on a different system with common component(s)). Include MBCRAs and address using the results to scope testing. If possible, use previous cyber test results for common components deemed sufficiently representative to reduce the scope of follow-on cyber testing. Also highlight any plans to expand previous testing during follow-on tests.

If the development consists of a new or upgraded component on a larger platform (e.g., a new radio on an aircraft or enhanced software functionality with a new external interface on a business system), identify any MBCRAs or cyber testing previously accomplished on the host platform that will establish a system cyber resilience assessment baseline. Also identify any testing performed on the system in support of another platform (e.g., the program will replace an aircraft's radar with one already installed and tested on another platform). If the development has been ongoing for many years, highlight only those key events from the previous two to three test events that may reduce cyber risk and be of interest to senior leaders and decision makers.

Do not discuss test results in this section of the TEMP or T&E strategy. Instead, identify where to find key cyber test results. Including specific cyber test results in the TEMP or T&E strategy may change the document's classification level.

K.2.6 T&E Management in the T&E Strategy

Describe the roles and responsibilities of key T&E personnel and organizations involved with cyber tests. Table K-2 describes T&E management responsibilities.

Table K-2. Cyber DT&E in Test and Evaluation Management

Responsibility	Description
Test and Evaluation (T&E) Organizational Construct	Identify the CyWG lead and consider specifying the CyWG membership. Specify the role the CyWG will play with respect to systems security engineering, and cyber test.
Common T&E Database Requirements	Describe the provisions for and methods of accessing, collecting, validating, transferring, and sharing cyber test data as it becomes available from system developer testing, government developmental and operational testing, oversight organizations, and any related supporting activities that contribute to or use cyber test data.
Deficiency Reporting	• Describe the deficiency reporting processes used to document and track cyber vulnerabilities and causal deficiencies identified during system development, developmental testing, integrated testing, concurrent testing, and operational testing. • Describe the deficiency rating system currently planned to assign deficiency or severity levels to identify cyber vulnerabilities. • Provide the location(s) for tracking all identified deficiencies. • Describe how the deficiency reporting database is different from the common T&E database, if appropriate. • Explain how personnel access and share the information, including all applicable T&E organizations. The processes should address problems or deficiencies identified during both system developer and government test activities.
Integrated Test Program Schedule	• Provide a quick summary of the integrated cyber test events planned, including:

Responsibility	Description
	– Integrated system developer–government testing in a system developer facility (see Section 1.6). – Integrated developmental test events that will incorporate tailored objectives to meet both developmental and operational test measures (see Section 1.6). – Concurrent cyber and non-cyber performance testing (see Section 1.7). – Government acceptance cyber T&E. • Include the level of integration and what each event will inform; explain the rationale for the decision; highlight why the CyWG thinks the test article will be sufficiently mature. • Explain any accepted risks related to limitations associated with the cyber test schedule.

K.2.7 Evaluation Framework Using the Integrated Decision Support Key

The IDSK is a framework developed and managed by the program manager. The IDSK provides a structured approach to identifying, collecting, and analyzing data to support informed decision making, acting as a roadmap connecting T&E activities to the information needs of decision makers. Creating the IDSK involves analyzing:

- Existing knowledge about the capability.
- Knowledge gaps that T&E will address.
- The timeline for when this information must be available to inform decisions

Figure K-1 depicts how the TEMP or T&E strategy will document the planned decisions, capabilities, and tests that inform the resources and scheduling of events.

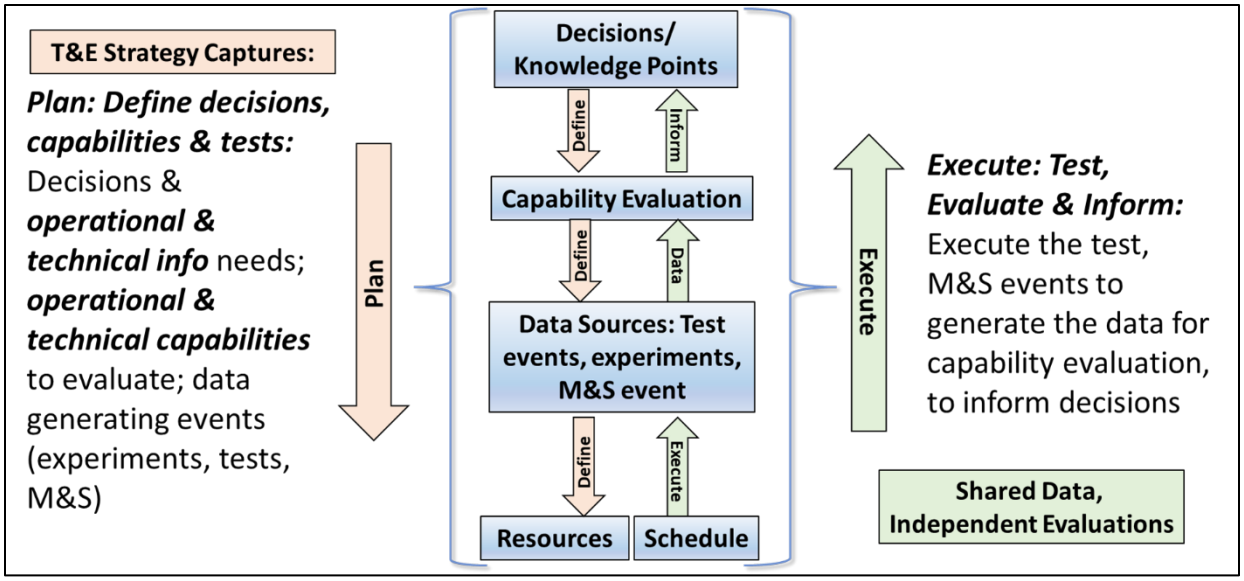


Figure K-1. IDSK for Better Decisions and Warfighter Capabilities

As depicted on the left side of Figure K-1, when developing or refining the IDSK, decision makers define their decisions or knowledge points and the questions underlying each decision point. The questions articulate the essence of the operational and technical capability knowledge needed by the decision maker to make the decision in an informed manner. The decisions and capability-focused questions form the "decision space" of the IDSK. Capability owners define the operational capabilities and the technical capabilities that enable designing and developing the system. These capabilities form the "evaluation space" of the IDSK. The team developing the IDSK defines the evaluation's data sources (e.g., wargames, experiments, M&S, and test events), providing the data for evaluation and decision support.

The right side of Figure K-1 **Figure K-1**represents executing the test events to generate the data, conducting the capability evaluation, and ultimately informing decisions.

The IDSK typically consists of a set of KPPs, KSAs, and other relevant evaluation criteria necessary to assess the performance, effectiveness, and suitability of a system or capability. DoW has not specified the format, decisions, or other details for an IDSK, enabling a fully tailorable approach by any program manager. An effort such as an Agile software pathway or DE approach could employ a "living IDSK" with a living T&E strategy as the source of truth with daily activities dynamically updating data enabling near real-time decision making.

Figure K-2 is one static IDSK construct depicting the necessary framework elements using a spreadsheet. The "decision space" decisions and associated operational/technical questions are in the top right two rows, forming the columns.

In Figure K-2, the operational capabilities with their measures and the technical capabilities with their measures are in the left-most columns, forming the rows. The team developing the IDSK may bin the capabilities into evaluation focus areas, for example, operational effectiveness with technical performance, SoS effectiveness with interfaces and interoperability, survivability with resilience (cyber resilience), and suitability with reliability and specialty engineering. Aligning and binning in this way illuminates integrated and concurrent cyber test opportunities.

The team places the data sources (M&S, tests, demonstrations, analysis, analysis, analysis, analysis, experiments, exercises, etc.) where needed to provide data for a capability evaluation.

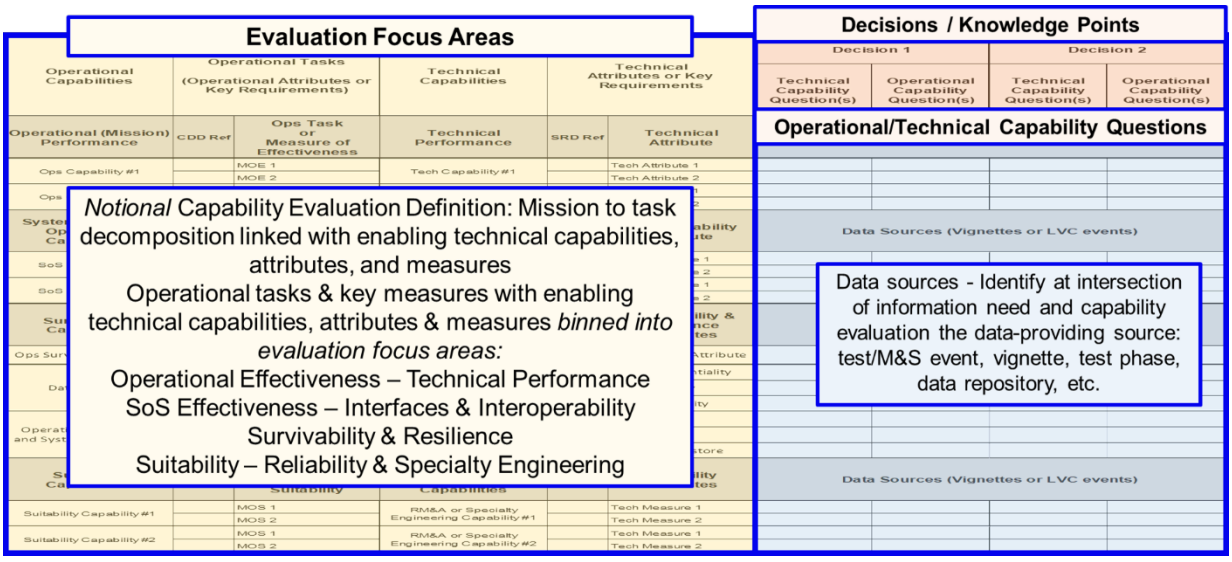


Figure K-2. IDSK Static Construct of Framework Elements

The CyWG is responsible for providing, refining, or updating cyber DT&E input to the IDSK. Continuous planning efforts and the entire cyber DT&E process should logically inform the priorities and essential data across the continuum of cyber DT&E necessary to inform the decisions. Figure K-3 depicts a notional cyber survivability section of an IDSK based on the construct in Figure K-2.

					Decision #1	Decision #2	...	Decision #N
Mission / Tasks & Operational Capabilities	**Description**		**Technical Capabilities**	**Description**				
ATO, IATT, etc.	Operational realism for network connectivity	Compliance	Cyber posture	Characterization of system cyber architecture and terrain				
PREVENT Ability to identify cybersecurity readiness and protect against cyber actions	Inherent and inherited cyber defenses of the system, including hardware, software, and firmware	Mission effects Cyber actions	Cybersecurity controls implementation, configuration, and architecture capabilities	Controls, cyber hygiene, and protections are implemented, up to date, maintained, and reflect ongoing changes				
MITIGATE Ability to perform system monitoring and detect cyber intrusions	Detection of cyberspace attacks and effectiveness of countermeasures (as applicable)	Mission effects Cyber actions	Cyber situational awareness	Metrics evaluating cybersecurity event alerts (e.g., number, percent detected, time to alert, accuracy of alert)				
RESPOND Ability to take response actions to mitigate the effects of cyber attacks	Response actions to cyberspace attacks and what effects those have upon operations	Mission effects Cyber actions	System mitigation and resilience actions	Response to cyber event (e.g., time, percent successful response, mission capability in degraded state)				
RECOVER/ADAPT Ability to recover, adapt, and restore system to operational state	Recovery of affected system functions and capability	Mission effects Cyber actions	System recovery and mission capability	Time to recover impacted system/mission from cybersecurity event to known good state, success of restoration				

Figure K-3. Notional Cyber Survivability Section of an IDSK

K.2.8 Cyber DT&E Strategy in the T&E Strategy

Outline the who, what, where, why, when, and how for planning, preparing, executing, evaluating, and reporting cyber DT&E. Describe the plan for iterative scoping activities that inform cyber DT&E including using threat intelligence, characterizing the attack surface, conducting MBCRAs, analyzing existing or known vulnerabilities, and using any prior testing results. Describe the general plans for regression testing and ICT supply chain testing. Explain the strategy for system developer testing, integrated system developer–government testing, and integrated developmental and operational testing (see Section 1.6).

K.2.9 Resources for Cyber Developmental Tests in the T&E Strategy

Identify the resource elements, both government and system developer, required to conduct cyber DT&E including funding; organizations; participants (system operators, inherent cyber defenders, external cyber defenders, test teams, etc., along with specific required expertise for execution and support); test articles; models and simulations; test facilities; test assets (tools, software, data collection, closed environments, cyber ranges, etc.); and related efforts such as VV&A. Specifically identify capabilities that the cyber teams do not already possess and should develop (attack tools for non-IP buses, threat-representative attack capability against specialized components such as cross-domain solutions; see the CUI Appendix L) and any system-specific capability (closed environments, cyber ranges, or other tools). Include long-lead items such as mission-representative cyber test assets. Describe any shortfalls, their impact(s) on planned cyber testing, and a plan to resolve or mitigate the identified shortfalls.

Table K-3 describes resources for cyber developmental tests. For test funding summary (bottom of Table K-3), there is no need to separately identify individual cyber events within a test category (e.g., if planning four cyber DT&E events to span over 2 fiscal years, enter all costs in a single cyber DT&E test line). If cost estimates are not available at the time of writing the strategy, identify the date when cost estimates for cyber testing will be available.

Table K-3. Resources for Cyber Developmental Tests

Test Resource Type	Description
Test Articles	• Cyber test artifacts needed to conduct the planned cyber test activities (e.g., cyber test assets, schematics). • Timing requirements for all test articles, including modeling and simulation (M&S). • Technical information required for each planned cyber test. • Subsystem (components, assemblies, subassemblies, or software modules) for individual testing, before testing in the final system configuration. • Quantities of test articles.
Specific Test Sites	• Cyber test ranges, facilities, and production systems used for each cyber test (e.g., system integration lab; cyber ranges; and distributed live, virtual, and constructive environments). • Timing for each range, facility, or system required to support the cyber test activities. • Required special characteristics.
Test Instrumentation	• Software or instrumentation acquired or built specifically to conduct the planned cyber tests (e.g., a capability to log system behaviors following a data integrity compromise). • Special tools or software that analysts or evaluators will need to read/pull data from the instrumentation.
Threat Representation	• Type(s)/level(s) of cyber threat actors emulated during cyber adversarial events if the security classification guide and the TEMP or T&E strategy's classification level permit. • The system data or prior test results available to the system developer and government developmental adversarial test teams for test preparation. • Resources required to emulate the anticipated threat environment and actors.
Test Article Sanitization and Expendables	• Basic plan to return identified cyber test assets to a known safe state following use. • Expendable cyber test assets that the test program will no longer use upon completion of the planned cyber test activities (typically due to classification and sanitization issues). • Plans for using and disposing of test assets.
Test Support Equipment	• Equipment required to conduct cyber tests. • Capabilities that cyber teams do not already possess and should develop (e.g., attack tools for non-Internet Protocol buses, threat-representative attack

Test Resource Type	Description
	capability against specialized components such as cross-domain solutions); see the CUI Appendix L. • Test locations requiring some form of test support equipment. • Emulators or other test support devices not included under the instrumentation requirements. • Special resources needed for data analysis and evaluation if required.
Models, Simulations, and Testbeds	• Models or simulations to support cyber test. • Models, simulations, and any hybrid tool (e.g., simulation over live system) used (per event), including computer-driven simulation models and hardware- and software-in-the-loop test beds. • Opportunities to simulate any of the required support. • Resources required for verification, validation, and accreditation of the models, simulations, and hybrid tool usage. • Resources required to validate and accredit M&S usage, the responsible agency, and timeframe.
Test Funding Summary	• Anticipated cost for government cyber developmental testing outlined in the strategy by fiscal year.

K.3 Cyber DT&E Information for Supplemental Cyber T&E Appendix

A supplemental cyber T&E appendix provides an opportunity for expanded discussion of details not already stated in the body of the T&E strategy. Detailed system architectures and diagrams are an example of the type of information for the appendix. The TEMP or T&E strategy needs a cyber appendix only if the main body does not enable including all needed information.

Glossary

The following terms are unique to this guidebook and are not defined in other official policies and guidance. For all other terms, see the glossary in DoWM 5000.103 or the WU Glossary (https://www.dau.edu/tools/dau-glossary).

attack surface analysis report. A document that identifies the logical and physical points of a system where an unauthorized user could attempt access; the report assesses the vulnerabilities and risks associated with those access points.

cyber DT&E teams. Refers specifically to system developers, third-party cyber test teams, government test organizations, and the personnel responsible for conducting cyber DT&E.

cyber T&E strategy. A comprehensive plan outlining how to assess the security and resilience of a system throughout its life cycle. It defines the methods, tools, and criteria used to verify the system's cyber requirements; identify, evaluate, and mitigate vulnerabilities; and verify that the system operates resiliently in its intended environment. The plan within the TEMP, or other T&E strategy, describes the organization's approach (who, what, where, when, and how) to verify and validate the performance, effectiveness, and security of the system against potential cyberspace threats.

FedRAMP. Provides a standardized approach for secure cloud services across Federal departments and agencies. It is mandatory for CSPs that process, store, or collect Federal information.

security control enhancements. Statements of security capability to (1) build in additional, but related, functionality to a basic control; and/or (2) increase the strength of a basic control.

stakeholders. The individuals, groups, or organizations that can affect a project's outcome, activity, or decision, or those that the project's outcome, activity, or decisions impact. The project may consult, inform, or be accountable to decisions involving cyber DT&E or the system under development, analysis, or test.

stimulus, stimulation. The set of input conditions and/or signals used to investigate the SUT's response in reaction to applied inputs or signals. A stimulus should be valid and controlled and should have acceptable residual risk.

technical security controls. The safeguards or countermeasures for an information system primarily implemented through engineering and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system.

Acronyms

3PAO	third-party assessment organization
AAF	Adaptive Acquisition Framework
AI	artificial intelligence
AISWG	Acquisition Intelligence Support Working Group
AO	authorizing official
API	application program interface
AT	anti-tamper
ATC	authorization to connect
ATO	authorization to operate
BOM	bill of materials
B/P/C/S	base/post/camp/station
CAC	common access card
CAD	Cyber Attack-Defense
CAP	cloud access point
CDD	Capability Development Document
CDRL	Contract Data Requirements List
CDT	chief developmental tester
CEEC	cyberspace effects and enabling capabilities
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CNAP	cloud-native access point
CNS	Capability Needs Statement
COI	critical operational issue
COLISEUM	Community On-Line Intelligence System for End Users and Managers
CONEMP	concept of employment
CONOPS	concept of operations
COR	contracting officer’s representative

COTS	commercial off-the-shelf
CPI	critical program information
CSA	cyber survivability attribute
C-SCRM	cyber supply chain risk management
CSO	cloud service offering
CSP	cloud service provider
CSS	cybersecurity strategy
CSSP	cybersecurity service provider
CTI	cyber threat intelligence
CTP	critical technical parameter
CUI	controlled unclassified information
CVE	common vulnerabilities and exposures
CVSS	Common Vulnerability Scoring System
CWE	common weakness enumeration
CyberDT XSWG	Cyber Developmental Test Cross-Service Working Group
CyWG	cyber working group
D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
DA	decision authority
DBS	defense business system
DCAT	DoW cyber assessment team
DCO	defensive cyberspace operations
DCRT	DoW Cyber Red Team
DCSA	Defense Counterintelligence and Security Agency
DCWF	DoW Cyber Workforce Framework
DE	digital engineering
DevSecOps	development, security, and operations
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DIB	defense industrial base

DID	data item description
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITL	Defense Intelligence Threat Library
DIV	Data and Information Viewpoint
DNS	Domain Name System
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	DoD directive
DoDI	DoD instruction
DoDIN	DoD Information Network
DoW	Department of War
DoWM	DoD manual
DR	deficiency report
DT	developmental test
DT&E	developmental test and evaluation
DTM	directive-type memorandum
EMSO	electromagnetic spectrum operations
EW	electronic warfare
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FFRDC	Federally Funded Research and Development Center
FOCI	foreign ownership, control, or influence
GOTS	government off-the-shelf
GPS	Global Positioning System
HAT TRICK	High Adversary Tier Threat Response Interdicting Cyberspace Kill-Chain
HBOM	hardware bill of materials
HFTA	heterogeneous fault-tolerant architecture
HWIL	hardware-in-the-loop

IaaS	infrastructure as a service
IAP	Internet access point
IC	intelligence community
ICAM	Identity, Credential, and Access Management
ICD	Initial Capabilities Document
ICT	information and communications technology
IDSK	Integrated Decision Support Key
IL	impact level
INCOSE	International Council on Systems Engineering
IoT	Internet of Things
IP	Internet protocol
IPC	Intelligence Production Center
ISP	Information Support Plan
ISSM	information system security manager
IT	information technology
ITT	integrated test team
JCIDS	Joint Capabilities Integration and Development System
JETEP	Joint Engineering and Test Enterprise Portal
JHU APL	Johns Hopkins University Applied Physics Laboratory
JIOR	Joint Information Operations Range
JMETC	Joint Mission Environment Test Capability
JMN	JMETC MILS Network
JRSS	Joint Regional Security Stacks
KPP	key performance parameter
KSA	key system attribute
LCSP	Life Cycle Sustainment Plan
LDTO	lead DT&E organization
M&S	modeling and simulation
MBCRA	mission-based cyber risk assessment

MBSE	model-based systems engineering
MCA	major capability acquisition
MILS	Multiple Independent Levels of Security
MIL-STD	Military Standard
MOA	memorandum of agreement
MOE	measure of effectiveness
MOP	measure of performance
MTA	middle tier of acquisition
NCIJTF	National Cyber Investigative Joint Task Force
NCRC	National Cyber Range Complex
NDI	non-developmental item
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	national security systems
NVD	National Vulnerability Database
O&S	operations and support
OACRA	Ontology for Attacks in Cyber Risk Assessments
OSD	Office of the Secretary of Defense
OSW	Office of the Secretary of War
OSS	open-source software
OT	operational test
OT&E	operational test and evaluation
OTA	operational test agency
OTO	operational test organization
OV	Operational Viewpoint
OWASP	Open Worldwide Application Security Project
P1	Platform One
PA	provisional authorization
PaaS	platform as a service

PATT	penetration and adversarial test team
POC	point of contact
POR	program of record
PPIP	Program Protection Implementation Plan
PPP	Program Protection Plan
PR	production request
PWS	Performance Work Statement
R&D	research and development
RACI	responsible, accountable, consulted, and informed
RF	radio frequency
RFI	request for information
RFP	Request for Proposal
RMF	Risk Management Framework
ROE	rules of engagement
RSDP	Regional Service Delivery Point
S&T	science and technology
SaaS	software as a service
SAP	Security Assessment Plan
SAR	Security Assessment Report
SBOM	software bill of materials
SCCA	Secure Cloud Computing Architecture
SCG	security classification guide
SCRM	supply chain risk management
SE	systems engineering
SEP	Systems Engineering Plan
SETA	Systems Engineering and Technical Assistance
SIL	system integration lab
SIPRNET	Secret Internet Protocol Router Network
SISO	Simulation Interoperability Standards Organization

SLA	service-level agreement
SLOC	source lines of code
SMART	specific, measurable, achievable, relevant, and time-bound
SME	subject matter expert
SOO	Statement of Objectives
SoS	system of systems
SOW	Statement of Work
SP	special publication
SPRS	Supplier Performance Risk System
SPS	System Performance Specification
SQL	structured query language
SRD	System Requirements Document
SRS	Software Requirements Specification
SS	system survivability
SSE	system security engineering
SSP	System Security Plan
STAT	scientific test and analysis techniques
STIG	Security Technical Implementation Guide
SUT	system under test
SV	System Viewpoint
SysML	Systems Modeling Language
T&E	test and evaluation
TAC	Threat Analysis Center
TCP	Transmission Control Protocol
TEMP	Test and Evaluation Master Plan
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
UAF	Unified Architecture Framework
UARC	University-Affiliated Research Center
UCA	urgent capability acquisition
UON	urgent operational need
UUV	unmanned underwater vehicle
V&V	verification and validation
VA	vulnerability analyst
VDP	Vulnerability Disclosure Program
VEX	Vulnerability Exploitability eXchange
VoF	verification of fixes
VOLT	Validated Online Lifecycle Threat
VPN	virtual private network
VV&A	verification, validation, and accreditation
WAA	waveform analysis application
WIPT	working-level integrated product team
WU	Warfighting Acquisition University

References

All DoW issuances (DoD directives, DoD instructions, and DoD/DoW manuals) referenced throughout this guidebook are available at https://www.esd.whs.mil/DD/DoD-Issuances/.

Application Programming Interface (API) Technical Guidance. Office of the Under Secretary of Defense for Research and Engineering, October 2023. https://www.cto.mil/wp-content/uploads/2023/11/API-Guide-2023.pdf

Cloud Computing Security Requirements Guide (CC SRG), January 28, 2025 2024. https://public.cyber.mil/dccs/dccs-documents/

Code of Federal Regulations, Title 32, Part 117

Cyber Survivability Endorsement (CSE) Implementation Guide. Version 4.0. Joint Staff J6, Deputy Director for Information Warfare Requirements Division, September 2025.

Data Item Description DI-MGMT-82140, "Naval Aviation Cybersecurity Test Plan," July 26, 2017.

Data Item Description DI-SESS-82433, "Cybersecurity Supply Chain Risk Management (C-SCRM) Software Bill of Material (SBOM) Requirements," January 19, 2024.

Data Item Description DI-SESS-82434 "Cybersecurity Supply Chain Risk Management Hardware Bill of Materials Requirement," January 19, 2024.

Defense Federal Acquisition Regulation Supplement, current edition.

Department of Defense (DoD) Cloud Native Access Point (CNAP) Reference Design (RD), Version 1.0, July 29, 2021.

Department of Defense Cyberspace Effects and Enabling Capabilities Test and Evaluation Standards Guidebook, August 1, 2024.

Department of Defense (DoD) Secure Cloud Computing Architecture (SCCA) Functional Requirements. Version 2.9. Defense Information Systems Agency, January 31, 2017.

Department of Defense Systems Engineering Plan (SEP) Outline. Office of the Under Secretary of Defense for Research and Engineering, May 2023. https://www.cto.mil/wp-content/uploads/2023/06/SEP-Outline-4.1.pdf

Department of Defense Technology and Program Protection Guidebook. Office of the Under Secretary of Defense for Research and Engineering, July 2022. https://aaf.dau.edu/storage/2024/08/TPP_Guidebook.pdf

Developmental Test Cyber Vulnerability Analysis Standards, November 10, 2020. https://go.intelink.gov/workforce

Directive-type Memorandum 24-001, "DoD Cybersecurity Activities Performed for Cloud Service Offerings," February 27, 2024.

DoD Cloud Strategy. Department of Defense, December 2018.

DoD Directive 5101.18E, "DoD Executive Agent for Printed Circuit Board and Interconnect Technology," June 12, 2016, as amended.

DoD Directive 5200.47E, "Anti-Tamper (AT)," September 4, 2015, as amended.

DoD Directive 5205.07, "Special Access Program Policy," September 12, 2024.

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020.

DoD Instruction 4140.01, "DoD Supply Chain Materiel Management Policy," March 6, 2019.

DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," February 2, 2024.

DoD Instruction 4630.09, "Communications Waveform Management and Standardization," November 23, 2020.

DoD Instruction 5000.61, "DoD Modeling and Simulation Verification, Validation, and Accreditation," September 17, 2024.

DoD Instruction 5000.82, "Requirements for the Acquisition of Digital Capabilities," June 1, 2023.

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended.

DoD Instruction 5000.86, "Acquisition Intelligence," September 11, 2020.

DoD Instruction 5000.88, "Engineering of Defense Systems," November 18, 2020.

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020.

DoD Instruction 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," December 31, 2020.

DoD Instruction 5000.97, "Digital Engineering," December 21, 2023.

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015, as amended.

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," February 16, 2024.

DoD Instruction 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements," December 21, 2021.

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended.

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022.

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended.

DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020.

DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004.

DoD Instruction 8585.01, "DoD Cyber Red Teams," January 11, 2024.

DoD Instruction O-3600.03, "Test and Evaluation of Cyberspace Effects and Enabling Capabilities," January 19, 2022.

DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended.

DoD Manual 8140.03, "Cyberspace Workforce Qualification and Management Program," February 15, 2023.

DoW Manual 5000.103, "Cyber Developmental Test and Evaluation," February 25, 2026.

Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

Federal Acquisition Regulation, current edition.

FedRAMP Penetration Test Guidance. Version 4.0. General Services Administration, March 4, 2024. https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance_public_comment.pdf

Guide to Writing Requirements. INCOSE-TP-2010-006-04. Revision 4. International Council on Systems Engineering, July 1, 2023. https://www.incose.org/docs/default-source/working-groups/requirements-wg/gtwr/incose_rwg_gtwr_v4_040423_final_drafts.pdf?sfvrsn=5c877fc7_2

Incorporating Test and Evaluation into DoD Acquisition Contracts. Defense Acquisition University, October 1, 2011. https://www.dau.edu/tools/incorporating-test-and-evaluation-dod-acquisition-contracts

Manual for the Operation of the Joint Capabilities Integration and Development System. Joint Staff J-8 Force Structure, Resources, and Assessment Directorate, October 30, 2021.

Military Standard MIL-STD-882E, "System Safety," September 27, 2023.

Military Standard MIL-STD-1553C, "Digital Time Division Command/Response Multiplex Data Bus," February 28, 2018.

National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," Revision 1, September 2012.

National Institute of Standards and Technology Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," Revision 2, December 2018.

National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, September 2020.

National Institute of Standards and Technology Special Publication 800-160, "Engineering Trustworthy Secure Systems," Volume 1, Revision 1, November 2022.

National Institute of Standards and Technology Special Publication 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," Revision 1, May 2022.

National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Revision 3, May 2024.

National Institute of Standards and Technology Special Publication 800-228, "Guidelines for API Protection for Cloud-Native Systems," June 2025. https://csrc.nist.gov/pubs/sp/800/228/final

Requirements for the Acquisition of Digital Capabilities Guidebook. Office of the Department of Defense Chief Information Officer, February 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/RequirementsAcquisitionDigitalCapabilitiesGuidebook.pdf

Scientific Test and Analysis Techniques Center of Excellence Report, "Scientific Test & Analysis Techniques for Software Testing," STAT COE-Report-05-2015, April 17, 2015, as amended. https://www.afit.edu/STAT/statcoe_files/STAT%20for%20Software%20Testing%20V2.pdf

Simulation Interoperability Standards Organization Cyber Data Exchange Model. https://www.sisostandards.org/news/670308/Publication-of-Cyber-DEM-BONES-and-EW-DEM-Study-Group-Final-Report.htm

Software Developmental Test and Evaluation in DevSecOps Guidebook. Office of the Under Secretary of Defense for Research and Engineering, January 2025. https://www.cto.mil/dtea/software/

State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation 2016. IDA Paper P-8005. Institute for Defense Analyses, November 2016. https://www.ida.org/research-and-publications/publications/all/s/st/stateoftheart-resources-soar-for-software-vulnerability-detection-test-and-evaluation-2016

Systems Engineering Guidebook. Office of the Under Secretary of Defense for Research and Engineering, February 2022. https://ac.cto.mil/wp-content/uploads/2022/02/Systems-Eng-Guidebook_Feb2022-Cleared-slp.pdf

Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Version 5.0. International Council on Systems Engineering, 2023. https://sebokwiki.org/wiki/INCOSE_Systems_Engineering_Handbook

Top Threats to Cloud Computing 2024. Cloud Security Alliance, August 5, 2024. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

United States Code, Title 10

Websites

CISA ICT Supply Chain Resource Library. https://www.cisa.gov/ict-supply-chain-resource-library

CISA Learning Management System. https://niccs.cisa.gov/training/cisa-learning

CJCS Directives Library. https://www.jcs.mil/Library/

Cloud Computing Security Requirements Guide. https://public.cyber.mil/dccs/dccs-documents/

Cybrary.
https://www.cybrary.it/catalog/

DCWF.
https://public.cyber.mil/wid/dcwf/

DCWF Qualification Matrices.
https://cyber.mil/cw/cwmp/qualifications-matrices/

DoW CIO Library.
https://dodcio.defense.gov/Library/

DoW Issuances.
https://www.esd.whs.mil/DD/DoD-Issuances/

DoW Cyber DT&E Guidance.
https://go.intelink.gov/Cyber_DTE

JETEP.
https://jetep.apps.dso.mil/

MITRE D3FEND.
https://d3fend.mitre.org/

National Initiative for Cybersecurity Careers and Studies Education and Training Catalog.
https://niccs.us-cert.gov/training

Organization for the Advancement of Structured Information Standards: Structured Threat Information Expression, and Trusted Automated Exchange of Intelligence Information.
https://www.oasis-open.org/2021/06/23/stix-v2-1-and-taxii-v2-1-oasis-standards-are-published/

SISO Standards Products.
https://www.sisostandards.org/page/StandardsProducts

STAT Center of Excellence.
https://www.afit.edu/STAT/

World Wide Web Consortium Data Activity.
https://www.w3.org/2013/data/

WU Adaptive Acquisition Framework.
https://aaf.dau.edu

WU Cybersecurity Training.
https://www.dau.edu/cybersecurity/training

WU DCWF Cybersecurity Playlists.
https://www.dau.edu/cybersecurity/cyber-playlist

WU SMART Goals Worksheet Tool.
https://www.dau.edu/tools/smart-goals-worksheet

WU Workforce Credentials.
https://www.dau.edu/credentials

Department of War Cyber Developmental Test and Evaluation Guidebook

Office of the Under Secretary of War for Research and Engineering
Office of the Assistant Secretary of War for Mission Capabilities
Office of the Deputy Assistant Secretary of War for Multi-Domain Joint Operations
Developmental Test, Evaluation, and Assessments
3030 Defense Pentagon
Washington, DC 20301-3030
osd.r-e.comm@mail.mil
https://www.cto.mil/dtea/

Distribution Statement A. Approved for public release. Distribution is unlimited.