Assessing DoD Mission Resilience: A Guide to Cyber DT&E

July 31, 2025

Sarah Standard
Cybersecurity/Interoperability Deputy Director
Developmental Test, Evaluation, and Assessments

UNCLASSIFIED – Cleared for Public Release by the DoD Office of Prepublication Security Review, 1 July 2025, Case **25-T-2436**

Policy and Guidance Status

- DoD Manual 5000.UY “Cyber DT&E” implements DoDI 5000.89 policy
  - Completed legal sufficiency review
  - Awaiting signature by the Under Secretary of Defense for Research and Engineering, Mr. Emil Michael
    - Available as soon as the issuance process allows
  - Draft is cleared for public release, contact: OSDRE-DTEA-Cyber@groups.mail.mil
  - When published, will be available on https://www.esd.whs.mil/dd/

- DoD Cyber DT&E Guidebook V3 – Published June 2025
  - Available at: https://aaf.dau.edu/guidebooks/ and https://www.cto.mil/dtea/cyber/

- Future: online digital DoD Cyber T&E Guidebook

Agenda

- Guidebook Introduction
- Practical Application: Emergency Enterprise System (EES)
  - Cyber Working Group (CyWG)
  - Iterative Cyber DT&E
  - CyWG Scoping Activities During Planning
- Streamlining with Digital Engineering
- Q&A

Cyber DT&E Guidebook V3 Outline (Eight Chapters)

1. Introduction
- Organization of this Guidebook
- Audience, Purpose, and Usage
- Applicability
- Terminology
- Cybers Policies and Guidance for Defense Acquisition Programs and Systems
- Integrating Cyber Testing
- Concurrent Cyber and Non-Cyber Testing
- Summary of Integrated and Concurrent Testing

2. Cyber DT&E Overview
- Iterative Planning, Preparing, Executing, Evaluating, and Reporting
- Cyber Working Group
- Early CyWG, Test Team, and Analyst Involvement
- Role of STAT in Cyber DT&E
- Cyber DT&E Relationship to System Security Engineering

3. Iterative Planning for Cyber DT&E
- Cadence
- Inputs
- Activity: Cyber DT&E Strategy Scoping
- Activity: CyWG Input to System Developer Contract Requirements
- Activity: Cyber DT&E Iterative Input to the TEMP or T&E Strategy
- Artifact Generation

4. Preparing for Cyber DT&E
- Inputs
- Activity: Gather Detailed Cyber DT&E Plan Information
- Activity: Develop the Test Plan
- Activity: Prepare for Cyber DT&E Events
- Activity: Conduct Cyber DT&E Readiness Reviews
- Artifact Generation

5. Executing Cyber DT&E
- Inputs
- Activity: Conduct Test
- Artifact Generation

6. Evaluating Cyber Developmental Test Data
- Input
- Activity: Cyber Developmental Test Evaluation
- Artifact Generation

7. Reporting Cyber DT&E Results
- Inputs
- Activity: Develop Cyber DT&E Reports
- Artifact Generation
- Evidence/Data Management

8. Cyber DT&E Process Challenges and Digital Engineering Considerations
- Non-Acquisition and Pre-Acquisition
- AAF Pathway Considerations
- Strategies for Tackling Cyber DT&E Process Challenges
- Model-Based Systems Engineering and Digital Engineering

Cyber DT&E Guidebook V3 Outline (13 Appendices)

- **Appendices**
  - A: Considerations for Staffing Cyber DT&E Activities
  - B: Examine and Advise on Cyber Performance Requirements and Measures for Cyber DT&E
  - C: Key System Artifacts for Cyber DT&E Analysis and Planning
  - D: Cyber Threat Assessment for Cyber DT&E
  - E: Attack Surface Characterization
  - F: ICT Supply Chain Cyber DT&E Considerations
  - G: Mission Based Cyber Risk Assessments
  - H: Cyber DT&E of DoD Systems Using Commercial Cloud
  - I: Incorporating Cyber DT&E into DoD Contracts
  - J: Cyber Developmental Test Infrastructure and Environment Planning
  - K: Cyber DT&E Strategy Considerations
  - **Publish separately**:
    - CUI Appendix L: Cyber DT&E of Specialized Assets (CAC Access)
    - Online Appendix M: Cyber DT&E for Artificial Intelligence Enabled Systems (AUGUST)
- **Acronyms, Glossary, and References**

Definitions

- Cyber DT&E: 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., during S&T.
- Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
- Operational resilience: The functionality enabling a system to resist, absorb, and recover from or adapt to an adverse occurrence **during operation** that may cause harm, destruction, or loss of ability to perform mission-related functions.
- Cyber resilience: The cyber component of operational resilience.

BLUF: Conduct Iterative Cyber DT&E Throughout Developmental Efforts

- Iterative and recursive verification of cyber resilient systems, and the evaluation of the system technical cyber risks impacting assigned missions
- Use current mission, threat, vulnerabilities to assess system's ability to:
  - Prevent cyberspace events from causing the degradation or failure of mission or safety critical functions or operational mission impacts
  - Detect anomalies caused by cyberspace events
  - Determine the cause of the anomaly, system misconfigurations, or design flaws
  - Report facts about the cyberspace event sufficient to mitigate the anomaly or design flaw to a responsible entity, which may be a non-person entity
  - Enable the entity to mitigate the reported anomaly both during and after the operational mission
  - Recover from the degradation or loss of mission or safety critical functions and maintain operational resilience in cyberspace throughout the system's life cycle

Measurable and testable cyber requirements aligned to achieving mission and surviving cyber threat

Software is never done, cyber risk never ends, continuous Planning scopes and prioritizes sustainment cyber DT&E

Key Features of the DoD Cyber DT&E Guidebook

- Flexibility and Customization
- Interdisciplinary Collaboration
- Organized Structure
- Agile and Iterative Methodology
- Focus on Emerging Technologies and Attack Surfaces
- Early and Continuous Assessment
- Data-Driven Decision Support
- Commitment to Workforce Development

Mission Assurance

Moving beyond simply protecting the system to ensuring the mission continues even if the system is compromised

Notional Example: Emergency Enterprise System (EES)

Primary Mission (PM) 1: Provide interoperable communication capabilities

PM 2: Manage emergency vehicle fleet

PM 3: Manage emergency response actions

- EES is critical for emergency response; real-time geolocation, vehicle health monitoring, dispatch capes
- Comprised of three main components
  - Cloud-based Integrated Vehicle Information and Logistics (CIVIL) (Cloud-based): The central management and data processing hub.
  - EM1 Gateway (GW): The interface for emergency vehicles, handling communication and data transmission.
  - EM1 Remote Terminal (RT): The user interface for authorized personnel to interact with the EES.

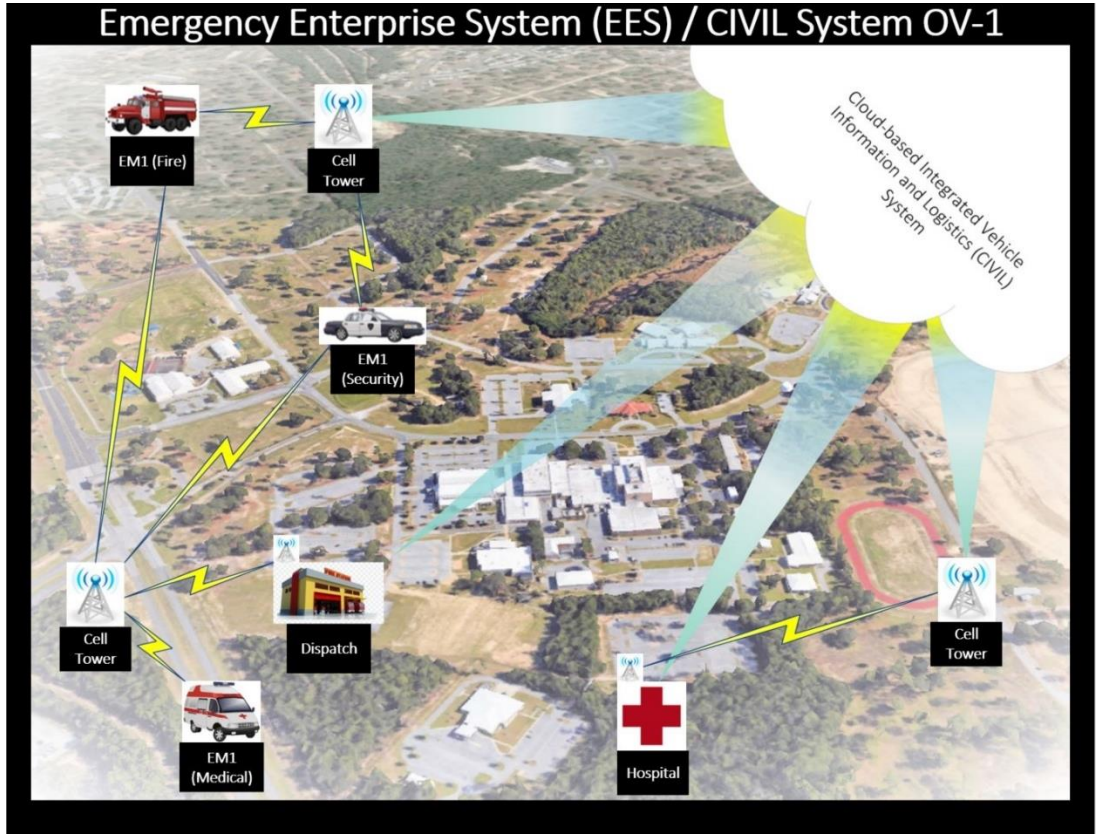


Image Source: EES notional image used throughout original artwork from USAF cyberspace test squadron USAF 48th Cyberspace Test Squadron

Compromising the EES could directly impact the speed and effectiveness of emergency response, potentially costing lives

Notional EES is Following the Defense Business System Pathway (DoDM 5000.UY)

Image Source: DoDM 5000.UY, page 49

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3	4	5
Establish and charter the CyWG	●				
Examine and advise on cyber requirements	●	●	●	●	○
Examine threat assessments and characterize attack surface	●	●	●	●	●
Support criticality and MRT-C analysis	●	↻	↻	↻	○
Conduct or update MBCRA		●		●	○
Develop or update cyber DT&E strategy			●	↻	↻
Determine test infrastructure, tools, and data requirements			●	↻	↻
Plan resources and schedule government DT&E			●	↻	↻
Include cyber DT&E requirements in each RFP and contract		●	↻	○	○
Review system developer (contractor) or government development and test environment, processes, and tools				●	↻
Analyze existing or known vulnerabilities		●	●	●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received				●	↻
Leverage all available and relevant test data for test planning and ensure all test data is made available for subsequent testing				●	●
Conduct test readiness reviews				●	●
Execute security verification throughout the system's life cycle			●	●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system				○	
Execute planned government acceptance cyber T&E				●	
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events				●	○
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies				●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01				●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●	●	●
Plan and update sustainment cyber DT&E activities and frequency			●	↻	↻

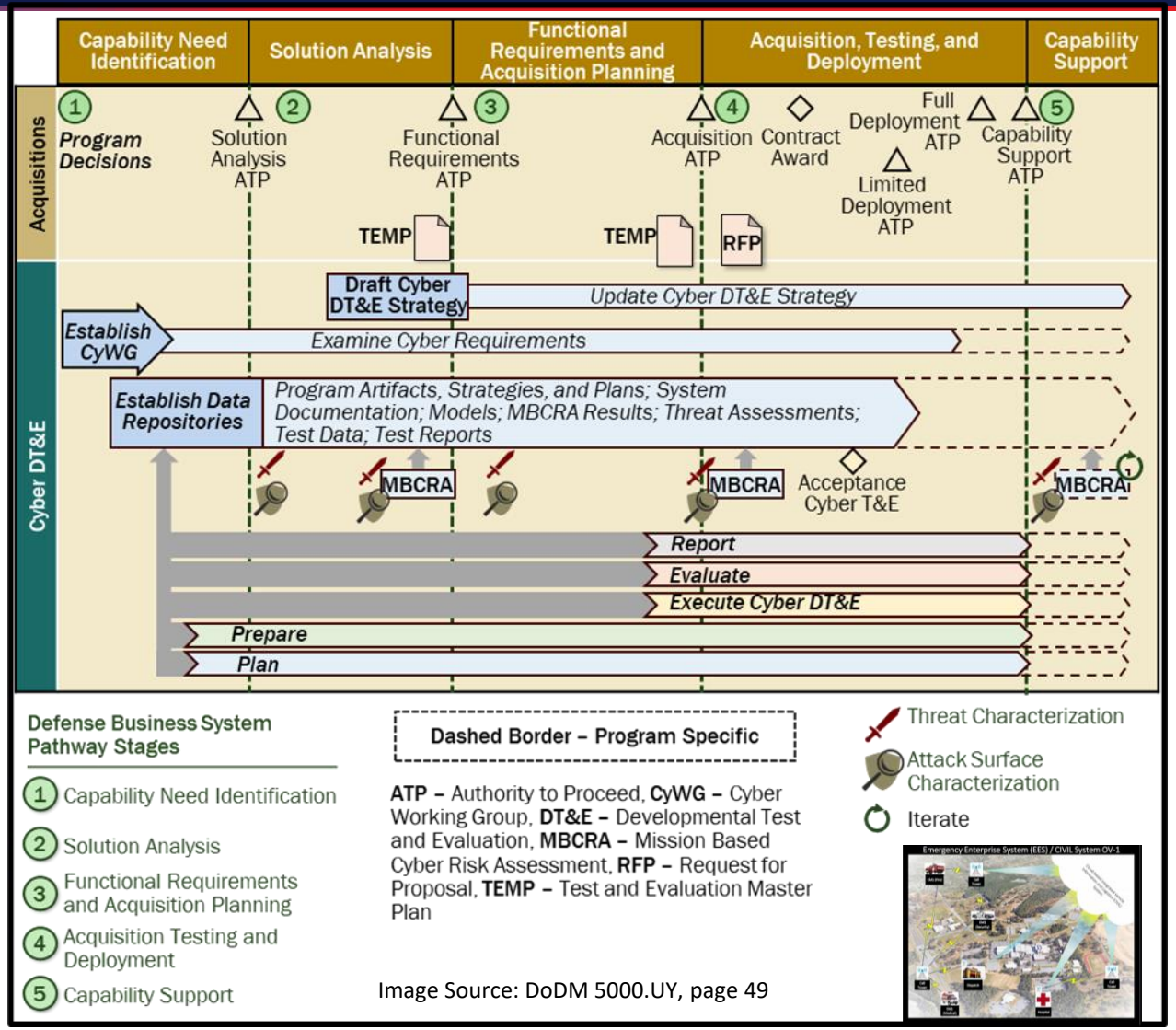
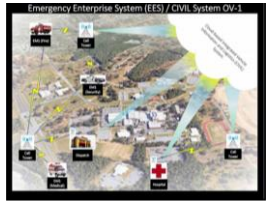
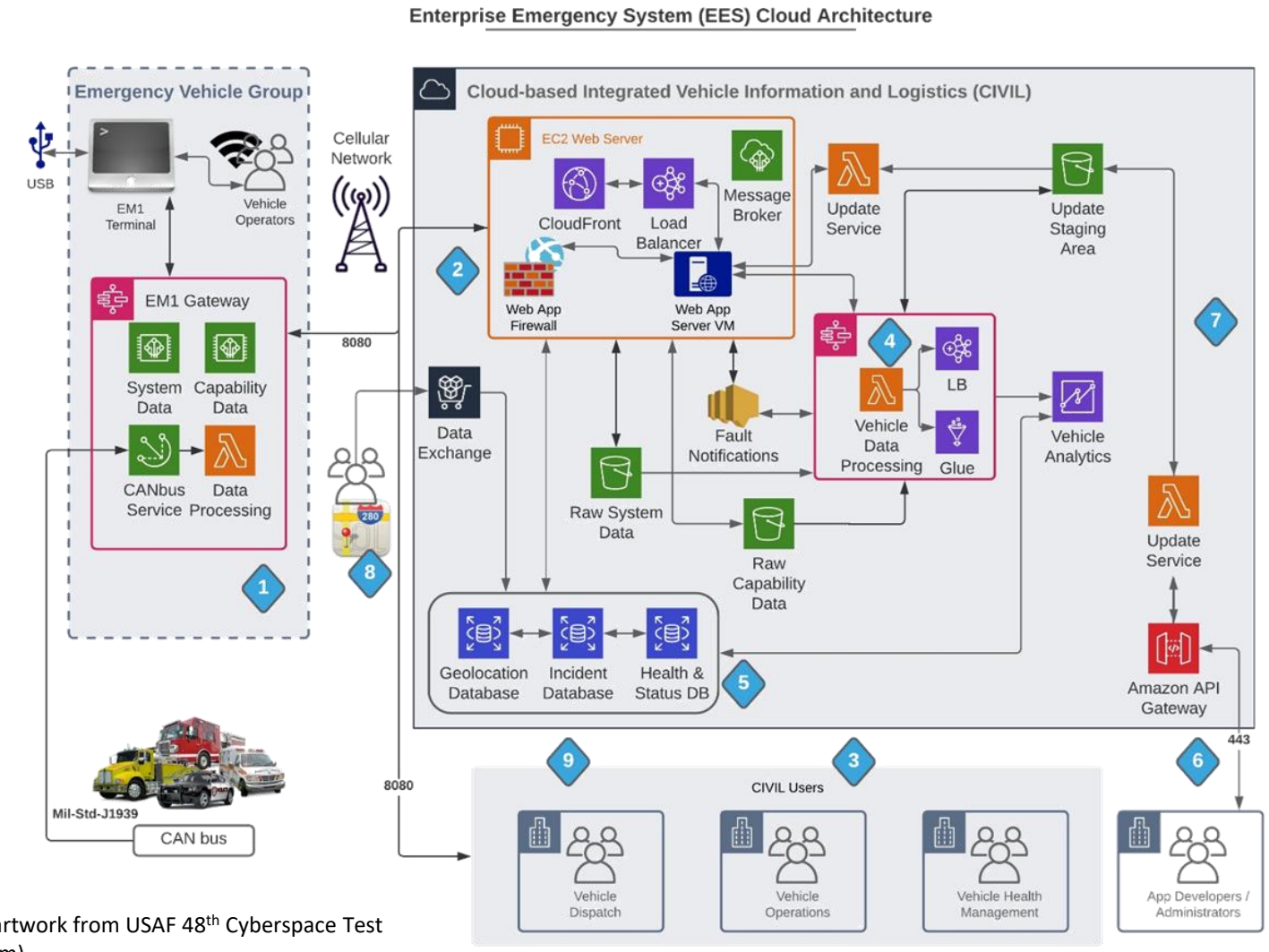


Image Source: DoDM 5000.UY, page 49

Image Source: 48th Cyberspace Test Squadron

Notional EES Cloud-Based Architecture





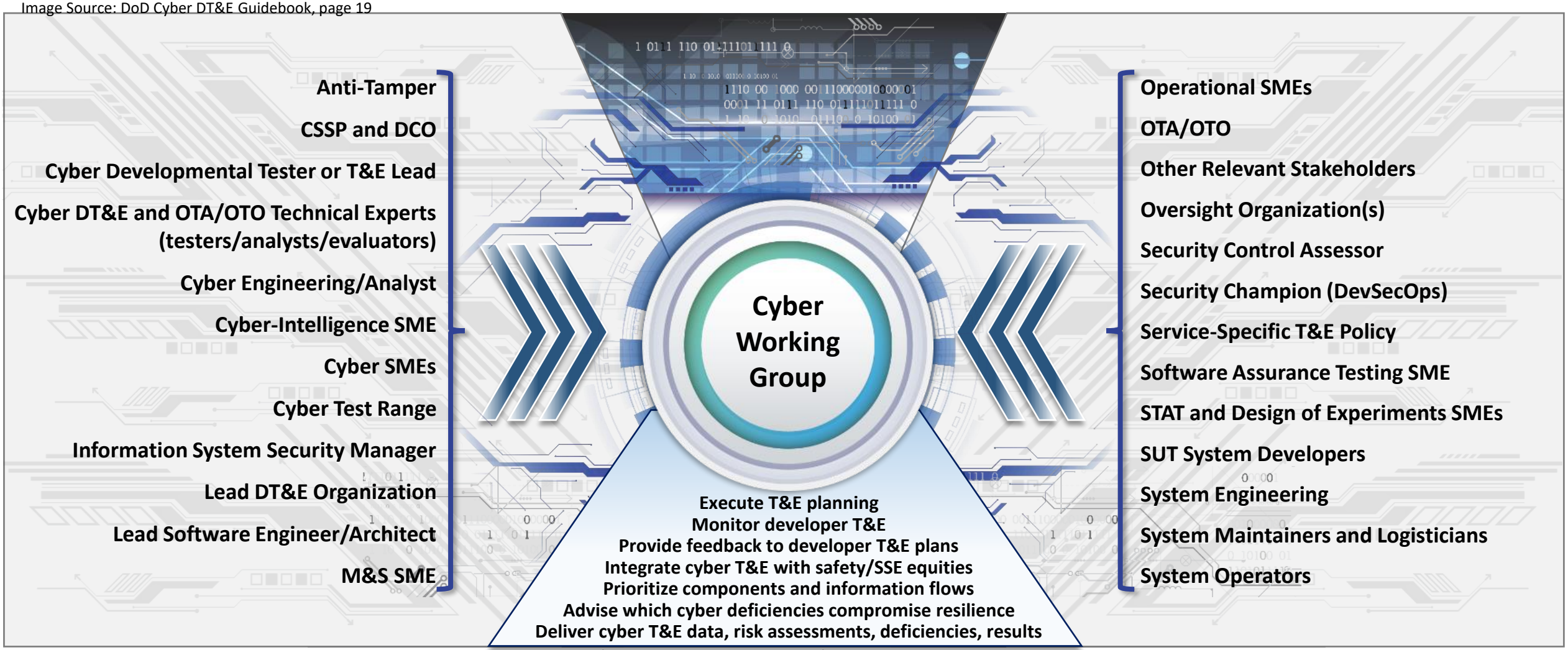
Process Flow

1. Vehicle health, status, and location data is collected by the client cloud service running on the EM1 unit on board and sent to CIVIL for processing.
2. Real-time events, raw system data, and raw capability data are transferred between vehicles and CIVIL.
3. System performance, health, and usage data is analyzed by Vehicle Dispatch, Vehicle Operations, and Vehicle Health Management personnel for system optimization and maintenance scheduling.
4. Vehicle health data is processed, stored, and analyzed to support maintenance requirements.
5. Vehicle system data is aggregated and stored in applicable relational databases.
6. App developers build new digital solutions for the connected ecosystem.
7. Updates and patches are deployed into the ecosystem for both the CIVIL application and the vehicle.
8. Real-time map and traffic data is received from third-party subscribtion services through the Data Exchange service.
9. Vehicle status and location data is monitored by Vehicle Dispatch. Vehicle dispatch uses availability data for emergency response taskings.

Images Source: Original artwork from USAF 48th Cyberspace Test Squadron (notional system)

Assemble and Charter the Cyber Working Group (CyWG)

Image Source: DoD Cyber DT&E Guidebook, page 19



CSSP: Cybersecurity Service Provider; DCO: Defensive Cyberspace Operations; OTA/OTO: Operational Test Agency/Operational Test Organization; M&S: Modeling and Simulation; SME: Subject Matter Expert; SSE: System Security Engineering; STAT: Scientific Test and Analysis Techniques; SUT: System Under Test

Appendix A: Staffing Cyber DT&E Activities

- Roles supporting cyber DT&E
  - Chief Developmental Tester or Test and Evaluation Lead
  - Cyber DT&E Leads
  - Cyber DT&E Technical Experts
  - Cyber Analysts
  - Other Subject Matter Experts (SMEs)
    - Cybersecurity SMEs
    - Intelligence SMEs
    - Operational SMEs
    - Software Assurance Testing SMEs
    - Secure Systems Engineering SMEs
  - Cybersecurity Vulnerability Analysts
  - Penetration and Adversarial Test Teams
  - DoD Cyber Red Teams
  - Cyber Test Range Representatives
  - System Developer Staff
  - Security Champion

Finding Cyber T&E Organizations

Use the Joint Engineering and Test Enterprise Portal (JETEP)

https://jetep.apps.dso.mil/cyber_te

Available on Platform One

1. Visit the Registration Page https://login.dso.mil/register
2. Fill out the Registration Form.
3. For CAC/IL4 access (required for JETEP): Use a .mil email address and leave the password fields blank until after account creation with a CAC.

Choose Participants Appropriate for Program Size and Scope

CyWG Guidance

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 EXECUTIVE 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

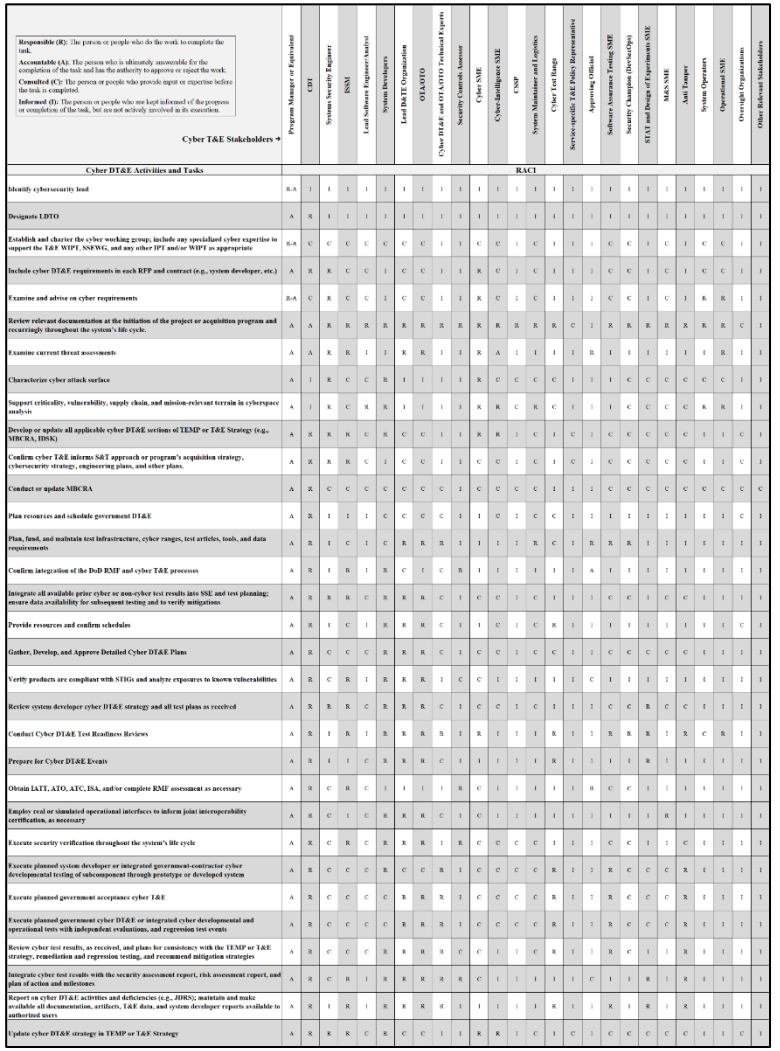
9.0 COORDINATION AND SIGNATURES

10.0 CONFLICT RESOLUTION

Section 2 contains an example CyWG Charter outline

Appendix A provides an example RACI (Responsible, Accountable, Consulted, and Informed) as both a figure and an embedded excel

Image Source: DoD Cyber DT&E Guidebook, page 18



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.

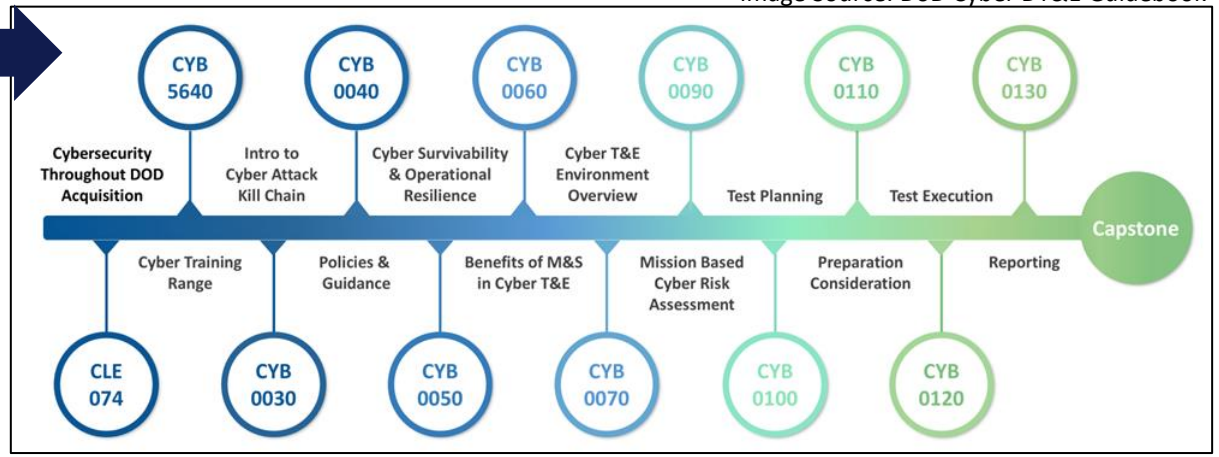
Cyber T&E Stakeholders → / Cyber DT&E Activities and Tasks	Program Manager or Equivalent	CDT	Systems Security Engineer	ISSM	Lead Software Engineer/Analyst	System Developers	Lead DT&E Organization	OTA/OTO	Cyber DT&E and OTA/OTO Technical Experts	Security Controls Assessor	Cyber SME	Cyber-Intelligence 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	MetA 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	I	C	C	I	C	I	I	I	C	C	I	C	I	C	C	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	I	C	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	C	I	R	R	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	I	R	I
Characterize cyber attack surface	A	I	R	C	C	R	I	I	I	I	R	C	C	C	C	C	I	I	I	C	C	C	C	C	C	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	C	R	R	I
Develop or update all applicable cyber DT&E sections of TEMP or T&E Strategy (e.g., MBCRA, ISSK)	A	R	R	R	C	R	C	C	I	I	R	R	I	C	I	C	I	C	C	C	C	C	C	I	I	C
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	C	I	I	C
Conduct or update MBCRA	A	R	C	C	C	C	C	C	C	I	C	C	C	C	C	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	I	C
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	A	I	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	C	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	C	I	I	I
Verify products are compliant with STIGs and analyze exposures to known vulnerabilities	A	R	C	R	I	R	R	R	R	I	C	C	I	I	I	I	I	C	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	C	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

Image Source: DoD Cyber DT&E Guidebook, page 119

Appendix A: Defense Acquisition University (DAU) Training

- Cyber T&E credential under development
- DAU cybersecurity training
  - https://www.dau.edu/cybersecurity/training
- Workforce Training Resources
  - DCWF: https://public.cyber.mil/wid/dcwf/
  - DCWF DAU Playlists:
    - https://www.dau.edu/cybersecurity/cyber-playlist
  - DCWF Qualification Matrices (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 over 3,000 cybersecurity and cybersecurity-related training courses.
  - Federal Virtual Training Environment:
    - https://fedvte.usalearning.gov
    - Provides free online cybersecurity training to U.S. government employees, federal contractors, and military Veterans.

Image Source: DoD Cyber DT&E Guidebook



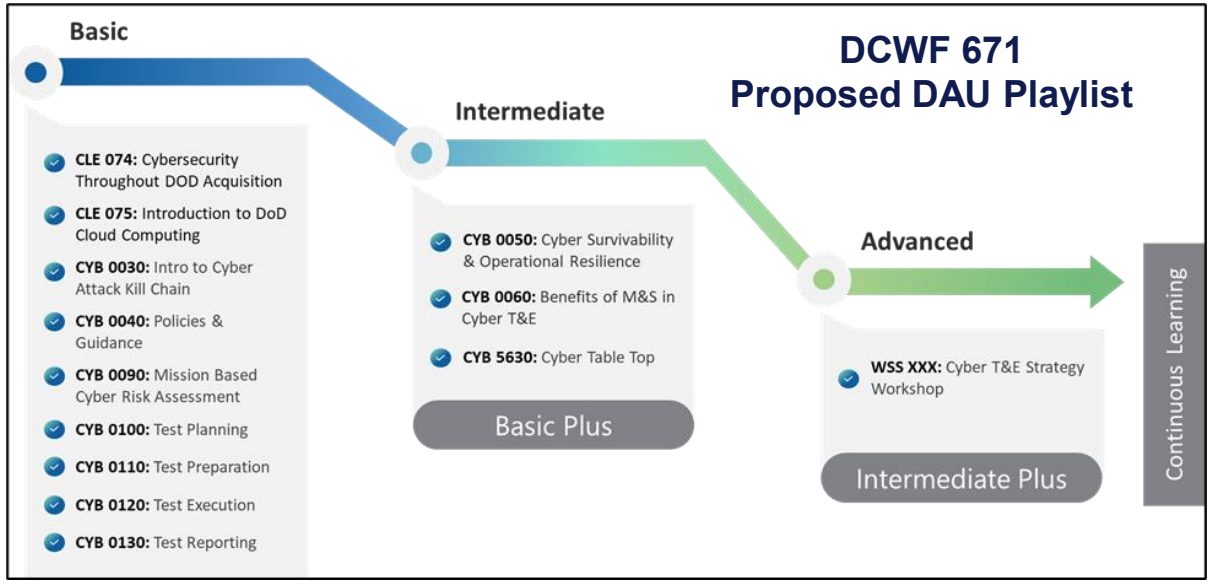


Image Source: DoD Cyber DT&E Guidebook, pages 102 and 103

Cyber DT Vulnerability Analyst Competency Maturity Model

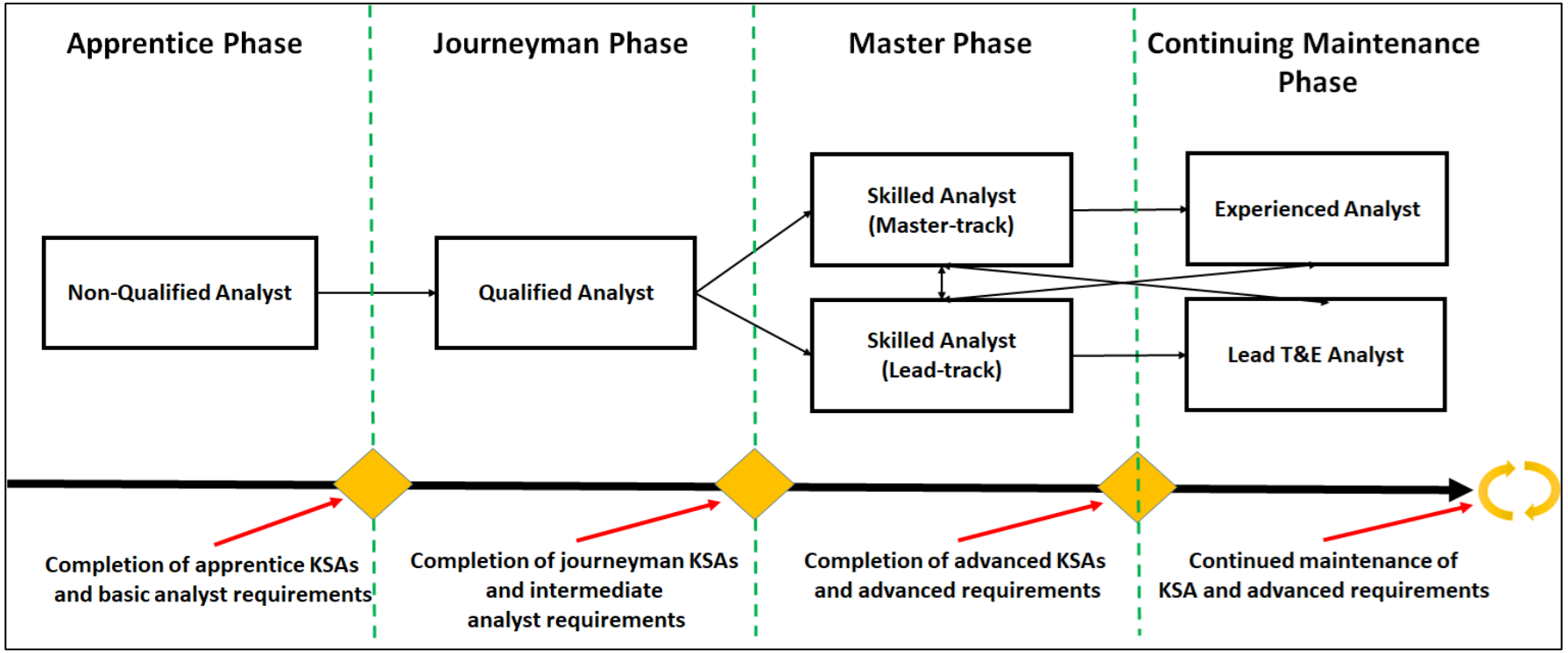


Image Source: DoD Cyber DT&E Guidebook, page 110

- Baseline Knowledge, Skills, and Abilities per level
- Published originally in 2018 and included in all versions of the guidebook starting in 2018
- Update underway
- Current content is available on Intelink:
  - Cleared for public release
  - Standards
  - Or contact DTE&A at OSDRE-DTEA-Cyber@groups.mail.mil

Maintaining Cyber DT&E proficiency – Developed by the Cyber DT Cross Service Working Group

Appendix B: Examine and Advise on EES Cyber Requirements (Notional EES Tier 1 Examples)

Image Source: 48th Cyberspace Test Squadron

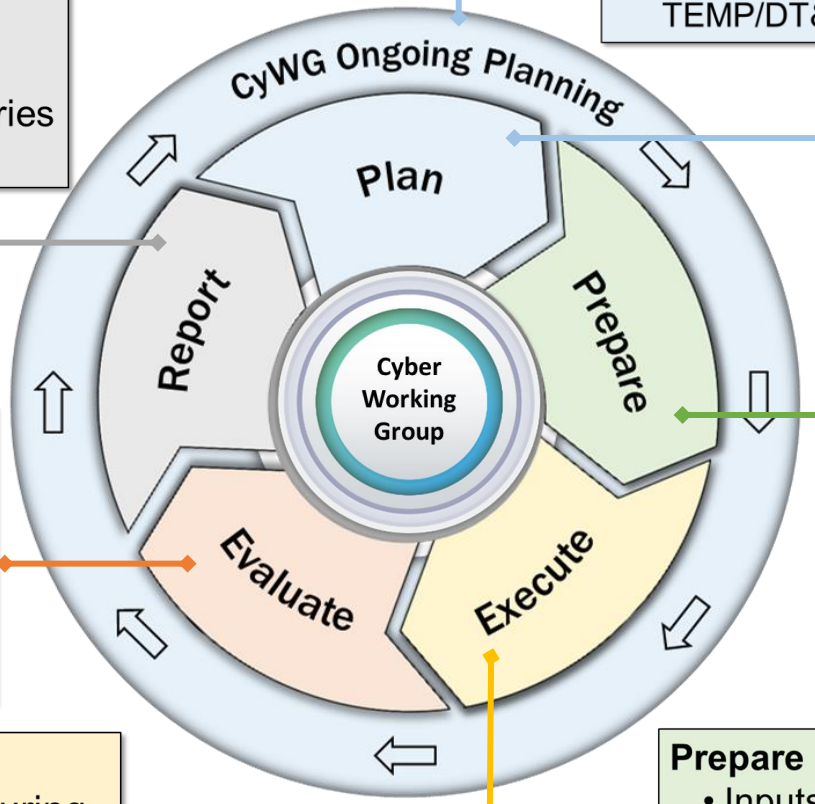
System-Level Requirement	Resilience Focus
1. Prevent unauthorized writing, modification, and transfer of data.	Data Integrity & Confidentiality, Recovery from Corruption
2. Prevent execution of unauthorized programs.	System Integrity, Containment of Malware
3. Enforce strict access control to system resources.	Least Privilege, Segmentation, Authentication
4. Prevent unauthorized data connections.	Network Segmentation, Intrusion Detection
5. Prevent introduction of unauthorized cyberspace assets.	Supply Chain Security, Integrity Verification
6. Resist unauthorized physical and logical access.	Hardening, Monitoring, Incident Response
7. Maintain mission capability despite system compromises.	Fault Tolerance, Redundancy, Graceful Degradation
8. Detect and report anomalous system behavior.	Threat Detection, Situational Awareness

Cyber DT&E Iterative Process

- No more six phases

Plan
- Ongoing throughout development, including during sustainment as cyber-enabled components, threats, and functionality change
- Cyber DT&E Strategy Scoping Activities
- Cyber DT&E Request for Proposal inputs
- Cyber DT&E Iterative Input to the TEMP/DT&E Strategy

Report
- Generate reports using data tables, classification guidance
- Deliver test reports to Authorizing Officials and program data repositories
- Informs ongoing CyWG Planning



Conduct iterative mission based cyber risk assessments (MBCRAs) in Plan

Evaluate
- Correlate findings with evidence and non-cyber tests
- Evaluate test data and measurements against cyber performance requirements

Execute
- Follow approved test plans ensuring freedom of maneuver and exploration to conduct discovery learning and gather test relevant insights
- Provide test data to independent evaluators

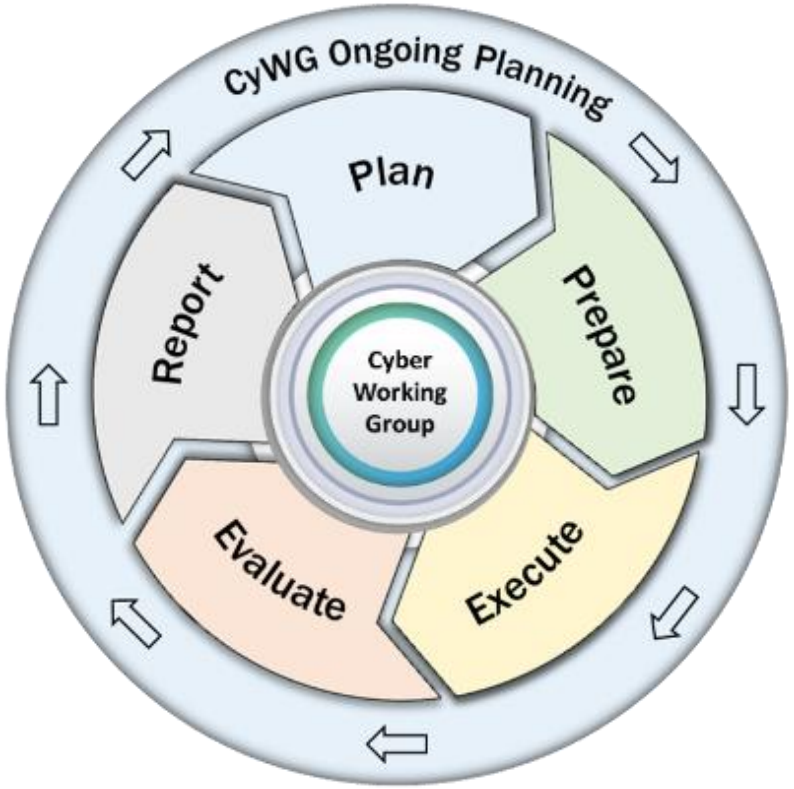
Prepare
- Inputs from CyWG ongoing Planning
- Develop Cyber DT&E Plans aligned to data tables
- Prepare for Cyber DT&E Events
- Cyber Developmental Test Readiness Reviews

Test-Fix-Test

Image Source: DoD Cyber DT&E Guidebook, page 14

Cyber DT&E is BOTH Iterative and Recursive

Iterative



Recursive – EES Example

Image Source: 48th Cyberspace Test Squadron

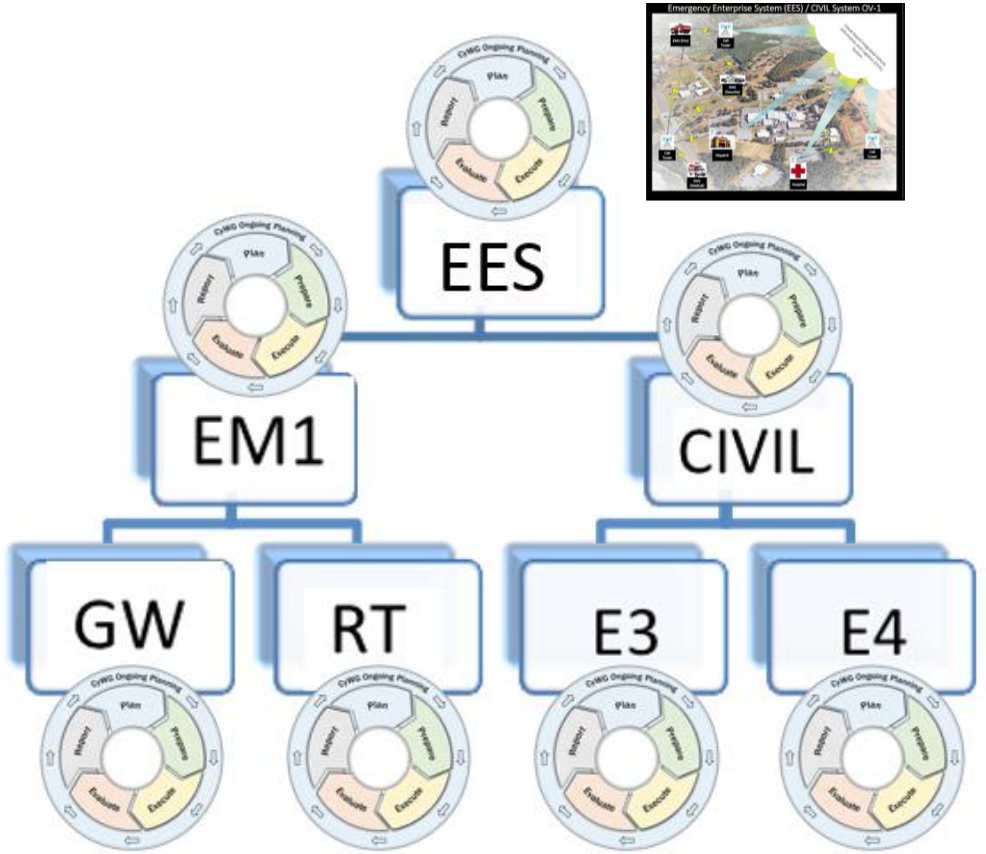


Image Source: DoD Cyber DT&E Guidebook, modified, page 15

Notional EES Intelligence Assessments (Appendix D) and Prior Testing

- Current intelligence indicates adversaries are highly interested in compromising cloud-based architectures
- Evidence confirms access credential and sensitive system information have been compromised by malicious actors
- Adversaries have knowledge of cloud web server enumeration tactics, techniques, and procedures
- Reports confirm adversarial activities against Controller Area Network (CAN) bus architecture, specifically Society of Automotive Engineers standard J1939, used in the emergency vehicle industry
- Evidence exists to confirm adversaries have already compromised similar systems through the CAN bus architecture

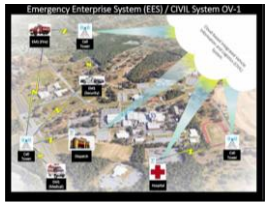


Image Source: 48th Cyberspace Test Squadron

- Evidence confirms adversarial use of remote code insertion through CAN bus architecture to affect remote terminal devices
- Adversary highly skilled in in the exploitation of air-gap media implementations
- Intelligence confirms adversary has a very sophisticated level of expertise, motivation, and opportunity to exploit systems using supply chains
- Adversary is well versed in packet analysis/spoofing techniques using Wireshark
- Field Programmable Gate Array (FPGA) reprogramming tactics, techniques, and procedures are well understood (conferences, published papers)
- Published test reports exist describing the ability of test agencies to remotely exploit CAN bus nodes and manipulate remote bus terminals

Initial Threat Informed Testing Priorities for Notional EES

- **Cloud Infrastructure Compromise**: Target cloud-based services, credential theft
- **CAN Bus Exploitation**: Exploit vulnerabilities in the J1939 protocol, remote code execution, FPGA reprogramming
- **Network Manipulation**: Packet analysis, spoofing, and interception
- **Supply Chain Compromise**: Target software patches for CIVIL, EM1 GW, and EM1 RT

- Configure simulation parameters to mimic attacker techniques, including simulating stolen cloud credentials, replay attacks, spoofing attempts, and denial-of-service attacks
- Test the system under varying network conditions and system load to ensure the performance constraints are consistently met for recovery objectives

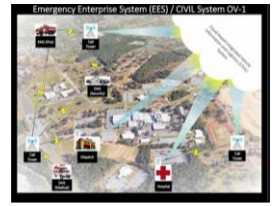


Image Source: 48th Cyberspace Test Squadron

Notional Criticality Analysis for EES Mission Relevant Terrain in Cyberspace (USAF approach)

Mission Decomposition / Critical Data Identification				Mission Impact Rating		
Critical Data Thread #	Primary or Secondary Mission (PM, SM)	Mission Critical Function or Safety Critical Function	Critical Data	Confidentiality	Integrity	Availability
1	PM 1: Provide interoperable communication capabilities	MCF 1: Establish/maintain connection between CIVIL and EM1 units	CIVIL Software Update Package	1	5	2
2	PM 1: Provide interoperable communication capabilities	MCF 2: Establish/maintain connection between CIVIL and authorized users	User Access Key IDs	1	2	5
3	PM 1: Provide interoperable communication capabilities	MCF 2: Establish/maintain connection between CIVIL and authorized users	User Secret Access Keys	5	2	5
4	PM 1: Provide interoperable communication capabilities	MCF 3: Provide remote CIVIL management	User Access Key IDs	1	2	5
5	PM 1: Provide interoperable communication capabilities	MCF 3: Provide remote CIVIL management	User Secret Access Keys	5	2	5
6	PM 2: Manage emergency vehicle fleet	MCF 4: Display real-time geolocation mapping	Traffic Light Metadata	1	5	5
7	PM 2: Manage emergency vehicle fleet	MCF 4: Display real-time geolocation mapping	EM1 Software Update Package	1	5	2
8	PM 2: Manage emergency vehicle fleet	MCF 5: Monitor emergency vehicle health and status	Vehicle Health & Status Data	3	5	4
9	PM 2: Manage emergency vehicle fleet	SCF 2: Emergency vehicle maintenance alerts and warnings	Vehicle Health & Status Data	3	5	4
10	PM 3: Manage emergency response actions	MCF 6: Process emergency incident notification	Incident Details	1	5	5
11	PM 3: Manage emergency response actions	MCF 7: Dispatch nearest available emergency vehicle to response location	Incident Details	1	5	5
12	PM 3: Manage emergency response actions	MCF 7: Dispatch nearest available emergency vehicle to response location	Vehicle Health & Status Data	3	5	4
13	PM 3: Manage emergency response actions	MCF 8: Synchronize routes between emergency vehicles and CIVIL	EM1 Access Key IDs	1	2	5
14	PM 3: Manage emergency response actions	MCF 8: Synchronize routes between emergency vehicles and CIVIL	EM1 Secret Access Keys	5	2	5
15	PM 3: Manage emergency response actions	MCF 8: Synchronize routes between emergency vehicles and CIVIL	Cellular Access Keys	5	2	5
16	PM 3: Manage emergency response actions	MCF 8: Synchronize routes between emergency vehicles and CIVIL	EM1 Software Update Package	1	5	2
17	PM 3: Manage emergency response actions	SCF 1: Traffic signal override	Traffic Light Algorithm	1	5	5
18	SM 1: Manage fleet health	MCF 9: Enable fleet maintenance scheduling	Scheduled Maintenance Plan	1	3	3

Critical Data, High Integrity: Vehicle Health & Status (includes location), EM1 and CIVIL Software Updates via CIVIL

Images Source: 48th Cyberspace Test Squadron

Notional EES Attack Surface Characterization and Threat Assessment Analysis (USAF Approach Extract) (Appendix E)

External Entity	Access Vector	First Cyber Susceptible Component (FCSC)	Data Flow Direction	Role Based Access Control (RBAC)	Network Access Control Lists (ACLs)	File System Access Control Lists (ACLs)	Technical Rating (1 - 5)	Technical Rating Synopsis	Threat Rating (1 - 5)	Threat Rating Synopsis
Vehicle CAN bus	EM1 RJ45 Ethernet Port	EM1 Gateway	Inbound	Yes	No	Yes	4	Attacks through this interface are highly feasible. CAN Bus technology in use does not provide ability to authenticate or validate input from external sources. If the exchange is legal and valid, it gets in. Tempered down to a 4 due to required access: physical or more sophisticated remote techniques.	5	Intelligence confirms adversary has a very sophisticated level of expertise in the exploitation of CAN Bus technology in use via physical and remote access.
USB Device	USB Port	EM1 Terminal	Bidirectional	No	No	No	1	Attacks through this interface are not possible. The USB ports on the EM1 Terminals are administratively disabled, physically destroyed with epoxy, and not intended to be used.	4	Intelligence confirms adversary has a sophisticated level of expertise in the exploitation of air-gap media implementations.
EM1 GW Vendor	Supply System	EM1 Gateway	Inbound	N/A	N/A	N/A	5	Attacks through this interface are highly feasible and successful supply chain exploits have been demonstrated by test agencies	5	Intelligence confirms adversary has a very sophisticated level of expertise, motivation, and opportunity to exploit systems using supply chains
EM1 RT Vendor	Supply System	EM1 Terminal	Inbound	N/A	N/A	N/A	5	Attacks through this interface are highly feasible and successful supply chain exploits have been demonstrated by test agencies	5	Intelligence confirms adversary has a very sophisticated level of expertise, motivation, and opportunity to exploit systems using supply chains

Appendix F: Supply Chain Cyber DT&E Considerations for Software Updates

Images Source: 48th Cyberspace Test Squadron

Conduct Initial MBCRA

Appendix G

The analytical process of identifying, estimating, assessing, and prioritizing risks based on impacts on DoD operational missions resulting from cyber effects on the system(s) being employed.

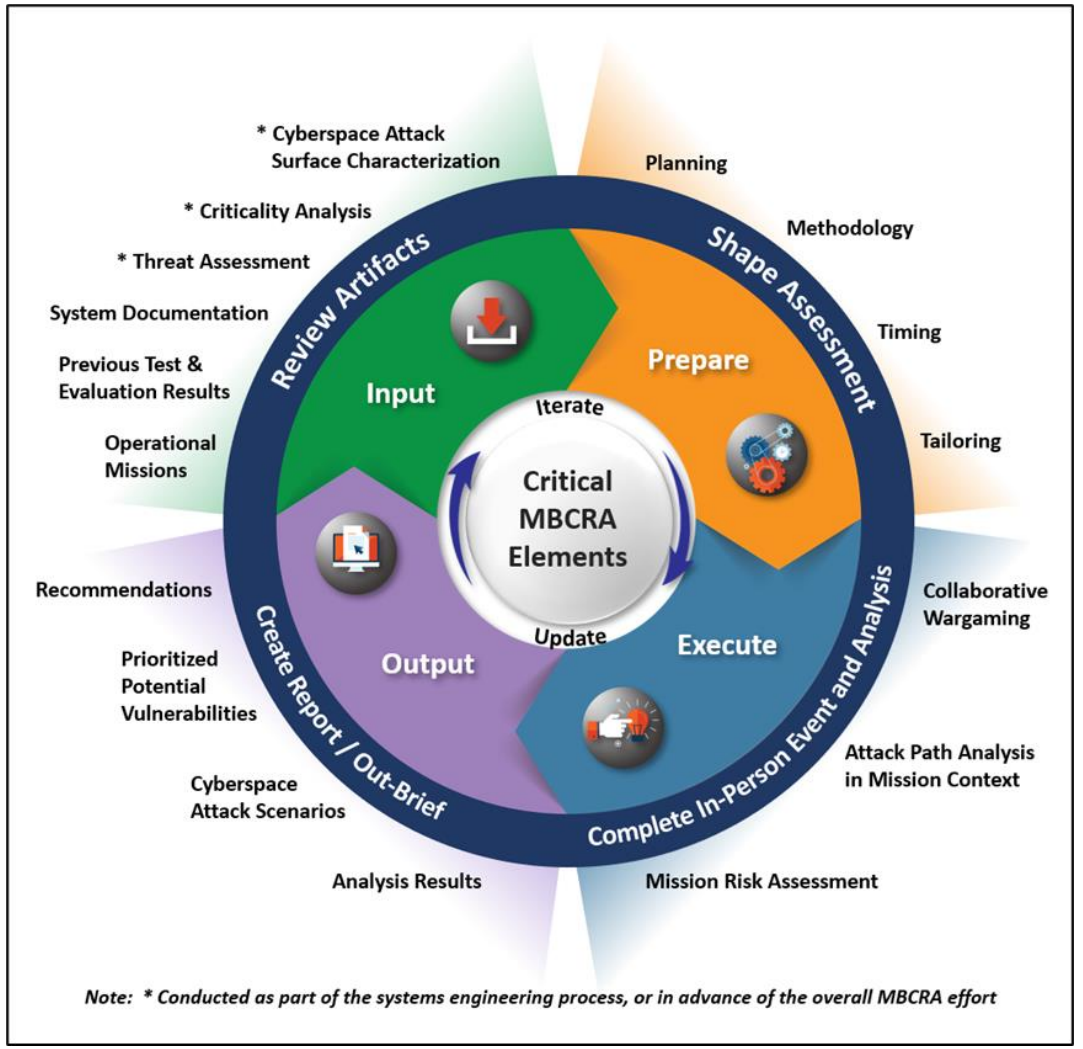


Image Source DoDM 5000.UY, page 23

Notional MBCRA EES Example Finding

- Malicious actor disables the EM1 Gateway navigation data to EM1 Terminal connection to deny the display of real-time geolocation information

- Impact PM 2: Manage emergency vehicle fleet

Image Source: 48th Cyberspace Test Squadron

- High Impact: Compromise through the EM1 Gateway Ethernet interface could result in injection of malicious logic, resulting in compromise of data confidentiality (sending data to unauthorized receiver), integrity (changing data), and/or availability (deleting or otherwise making data unavailable). Denying the availability of navigation and geolocation data could have multiple severe or catastrophic mission effects in the EES (e.g., unable to view communications or navigation data)

Initial CyWG Notional EES Attack Surface and Test Priorities

- Attack surface* priorities – Appendix E:
  - Commercial cloud service (**Appendix H**)
  - DoD Infrastructure and Enterprise Services
  - Inter- and Intra-System Architecture Network Interfaces
  - Interfaces with Interagency
  - Real-Time, Safety-Critical Systems (**Appendix L**)
  - Software Factories
  - Supply Chain (**Appendix F**)
  - System Architecture and Design Choices

* See DoD Manual 5000.UY Table 1

- Test priorities
  - **Degradation Modes:** How the system will function when compromised
  - **Redundancy/Failover:** Mechanisms to switch to alternative operation
  - **Isolation:** Limiting the impact of a compromise
  - **System Resilience, Recovery:** Returning to full functionality
  - **Data Integrity:** Detection of data manipulation
  - **Cyber-Electromagnetic Warfare**: Jamming, spoofing, interference, side channel, fault injection, position, navigation, and timing attacks (Appendix L)

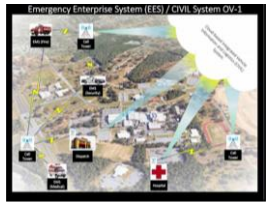


Image Source: 48th Cyberspace Test Squadron

Notional EES Requirement Decomposition with Measures and Allocation to EM1 Subsystem (Tier 2)

Image Source: 48th Cyberspace Test Squadron

- **EM1-7.1** Degradation: Upon detection of a compromise (e.g., unauthorized code execution, data corruption), the EM1 system shall degrade gracefully to a "Limited Functionality Mode" within 60 seconds.
- **EM1-7.2** Location Reporting: In Limited Functionality Mode, the EM1 system shall continue to transmit vehicle location data with a maximum latency of 10 seconds.
- **EM1-7.3** Vehicle Status: In Limited Functionality Mode, the EM1 system shall continue to transmit critical vehicle status with a maximum accuracy of +/- 5%.
- **EM1-7.3** Communication: In Limited Functionality Mode, the EM1 system shall maintain basic emergency communication capabilities with a success rate of 90%.
- **EM1-7.4** Isolation: A compromise of the EM1 RT shall not prevent the EM1 GW from communicating with other vehicles or CIVIL within 5 seconds.
- **EM1-7.5** Recovery: The EM1 system shall automatically attempt to restore full functionality within 15 minutes of compromise mitigation.
- **EM1-7.6** Compromise Detection: The EM1 system shall detect and log suspected compromise attempts with 95% accuracy.

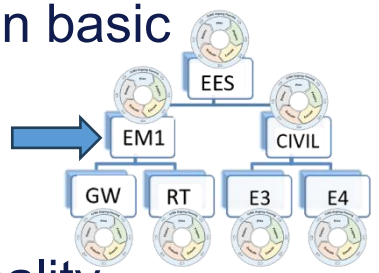


Image Source: DoD Cyber DT&E Guidebook, modified, page 15

Maintain mission capability despite system compromises

Notional EM1 Requirements Decomposition with Measures and Allocation to Components (Tier 3)

- **GW Degradation**: GW responsible for initiating Limited Functionality Mode based on compromise detection. (60 s)
- **GW Location Reporting**: GW responsible for forwarding location data from RT (even in Limited Functionality Mode). (10 s)
- **GW: Isolation**: GW responsible for maintaining communication with other vehicles/CIVIL despite RT compromise. (5 s)
- **GW Compromise Detection**: GW responsible for monitoring RT behavior and detecting anomalies. (95% accurate)
- **GW-Specific Requirement**: GW shall maintain a secure, isolated communication channel with CIVIL for reporting compromise events.

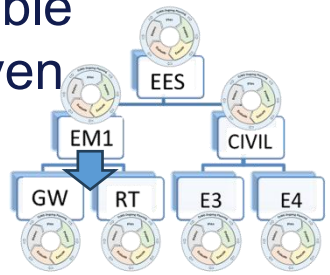
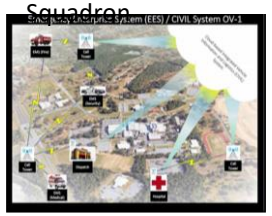


Image Source: DoD Cyber DT&E Guidebook, modified, page 15

Image Source: 48th Cyberspace Test Squadron



- **RT Degradation**: RT responsible for entering a reduced functionality state upon compromise detection. (60 s)
- **RT Vehicle Status**: RT responsible for continuing to collect and transmit critical vehicle status in Limited Functionality Mode. (100% pass)
- **RT Communication:** RT responsible for maintaining basic emergency communication in Limited Functionality Mode. (100% pass)
- **RT-Specific Requirement**: RT shall implement a secure boot process to prevent unauthorized firmware execution. (100% pass)
- **RT-Specific Requirement**: RT shall have a tamper-evident enclosure to detect physical compromise.

Maintain mission capability despite system compromises

Notional EES Test Teams Identify Test Techniques

- Simulate RT compromise and verify GW initiates Limited Functionality Mode
- Verify location data transmission during simulated RT compromise
- Simulate RT compromise and verify continued communication
- Inject malicious traffic from RT and verify GW detection
- Verify secure reporting channel
- Simulate compromise on RT and verify transition to Limited Functionality Mode
- Verify vehicle status transmission during simulated compromise
- Verify emergency communication functionality during simulated compromise
- Attempt to load unauthorized firmware
- Attempt to physically tamper with the device

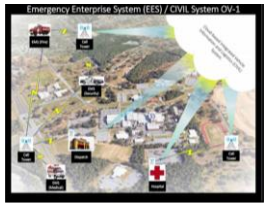


Image Source: 48th Cyberspace Test Squadron

Notional EES Testability Considerations & CyWG Focus

- Compromise Simulation: Develop realistic compromise scenarios (e.g., CAN bus attacks, remote code execution, data injection) to test these requirements
- Automated Testing: Automated testing is essential for verifying these requirements repeatedly and efficiently
- Performance Monitoring: Monitor performance metrics (latency, accuracy, success rate) during simulated compromises
- Fault Injection: Introduce faults (e.g., network disruptions, data corruption) to test the system's resilience

Key Measurable Outputs for the CyWG:

- Time to Degradation: How quickly does the system enter Limited Functionality Mode?
- Data Loss: How much data is lost during a compromise and recovery?
- Communication Availability: What percentage of communication is maintained during a compromise?
- Detection Rate: How accurately does the system detect compromise attempts?
- Recovery Time: How long does it take to restore full functionality?

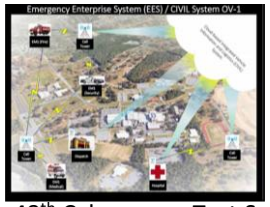


Image Source: 48th Cyberspace Test Squadron

Appendix I: Highlights to Provide Inputs to the RFP and Contract

Tailorable language examples: If it is not in the contract, do not expect to get it!

- Contractual Elements

- Section C:
  - Support to government led cyber DT&E
  - Support for MBCRA
  - Support government test planning
  - Contractor test requirements
  - Integrated contractor and government cyber testing
  - Contractor support for government cyber acceptance testing
  - Contractor cyber DT&E skillset and qualifications
  - Contractor testing for cloud systems
  - Contractor software testing
  - Contractor prototype testing
- Section F: Deliveries or Performance
- Section L: Instructions to Offerors or Respondents
- Section M: Evaluation Criteria

- Cyber DT&E Deliverables
- Contract Incentives

Notional EES RFP Required Tests (DoDM 5000.UY Table 2) (1)

Image Source: 48th Cyberspace Test Squadron

Test Type	Supporting EM1 Reqts.	Focus/Metric	RFP Deliverables
Architectural Vulnerability Assessment	All	Identify inherent weaknesses in design.	Detailed report of architectural vulnerabilities, mitigation plans.
Bug Bounty	All	Crowd-sourced vulnerability discovery.	Bug bounty program report, vulnerability disclosures, remediation status.
Controls Testing	EM1-7.1., 7.3	Verify security control effectiveness.	Test plans, results, and evidence of control functionality.
Interface Testing	EM1-7.2, 7.4	Assess interaction risks between EM1 components & external systems.	Test reports, identified vulnerabilities, and remediation plans.
MBCRA Verification	All	Validate findings from Mission Based Cyber Risk Assessment.	Test reports validating MBCRA findings, performance impacts during attack.

Notional EES RFP Required Tests (DoDM 5000.UY Table 2) (2)

Image Source: 48th Cyberspace Test Squadron

Test Type	Supporting EM1 Reqts.	Focus/Metric	RFP Deliverables
Network Vulnerability Assessment	EM1-7.4	Identify network-level weaknesses.	Network vulnerability scan reports, remediation plans.
Non-IP Device and Component Testing	EM1-7.3	Secure embedded systems & protocols.	Test reports, hardware data extraction attempts, interface security analysis.
Platform and Component Hardening Verification	All	Verify secure configuration of hardware & software.	Hardening checklists, configuration reports, patch management process documentation.
Recoverability Testing or Continuity of Operations Testing	EM1-7.5	Demonstrate recovery from compromise.	Recovery test plans, results, and documented recovery timelines.

Notional Government EES Acceptance Cyber T&E and Cyber DT&E

Test Type	Reqt	Focus	Test Needs
Cloud Testing	All	Verify security in a cloud environment	Cloud environment access, test data
Critical Infrastructure Assessment	EM1-7.1	Assess impact of external dependency failures	Dependency mapping documentation, simulation tools
Cyber-EMSO Testing	EM1-7.2, 7.3	Assess RF vulnerabilities	Spectrum analyzers, software defined radios, antennas
Cyberspace Kill Chain Testing	All	Simulate realistic attacks	Dedicated test network, attack tools, indicators of compromise database
Incident Response Testing	EM1-7.1, 7.5, 7.6	Evaluate incident response effectiveness	Incident response plan, simulation scenarios, test personnel
Concurrent Cyber and Non-Cyber Testing	All	Integrated adversarial testing	Integrated test environment, threat representative tools, safety protocols
Penetration Testing or Exploitation Analysis	All	Identify exploitable vulnerabilities	Dedicated test network, penetration testing tools, authorized access
Purple Team Testing	All	Collaborative testing to improve defenses	Integrated test environment, defined rules of engagement, communication channels

Image Source: 48th Cyberspace Test Squadron

Appendix J: Infrastructure Planning Highlights

- Cyber DT&E test infrastructure planning considerations
  - Development-test labs and software integration labs
  - Enabling adversarial testing – closed loop cyber test ranges
  - Building representative contested cyber environments

- Requesting virtual, restorable images and test articles to support early government cybersecurity and cyber resilience testing in lab environments

- MBCRA infrastructure considerations

- Infrastructure plan inputs for the T&E strategy

Notional Test Assets and Infrastructure in EES RFP

Image Source: 48th Cyberspace Test Squadron

- Dedicated Test Network: A physically isolated network mirroring the operational environment
- EM1 System Instances: Full EM1 system instances (GW & RT) for testing, including emulated system for government use on the National Cyber Range Complex
- Test Data: Realistic test data, including vehicle location, status, and communication logs
- Configuration Management Tools: Access to tools used to configure and manage the EM1 system
- Logging & Monitoring Tools: Access to system logs and monitoring data
- Vulnerability Scanning Tools: Access to vulnerability scanning tools used by the developer
- Secure channels for data transfer and communication during testing
- Comprehensive system documentation, including architecture diagrams, interface specifications, and security configurations
- Access to Source Code: (Potentially, depending on contract terms) Access to source code for white-box testing
- Hardware Access: Access to the RT hardware for physical security testing.
- Simulation Tools: Tools for simulating network disruptions, data corruption, and other compromise scenarios

Notional EES Verification of MBCRA Scenario Test (Prepare, Execute, Evaluate, Report: Sections 4-7)

Image Source: 48th Cyberspace Test Squadron

- **Test Case**: Simulate CAN bus attacks. Measure detection and isolation. Simulate a complete loss of communication with the compromised vehicle to assess recovery. Verify GW initiates Limited Functionality Mode. The target initiation time is < 5 seconds.
- **Requirements**
  - EM1-7.1 (Degradation – GW)
  - EM1-7.2 (Location Reporting - GW)
  - EM1-7.4 (Isolation - GW)

- **Mission impact summary**
  - Compromised vehicle data could result in unnecessary vehicle downtime, incorrect dispatch decisions, and endangering responders and victims
  - Recovery testing focuses on the system's ability to recover despite the compromise

Notional EES Supply Chain Attack Test (Prepare, Execute, Evaluate, Report: Sections 4-7)

Image Source: 48th Cyberspace Test Squadron

- **Test case**: Simulate a compromised software update/patch being deployed from the developer environment to CIVIL
  - Patch contains malicious code designed to alter vehicle data
  - Deploy the patch to the EM1 GWs
  - Detect malicious behavior (or not)
  - Simulate a catastrophic failure of the compromised EM1 GWs
- **Metrics** (verify all EM1 requirements)
  - Correlate metrics across components
  - Ensure the test environment accurately simulates the production environment
  - Run tests multiple times to ensure consistent results
  - Automate metric collection and analysis wherever possible
- **Mission impact summary**
  - Successful supply chain attack could compromise the entire fleet, resulting in significant operational downtime and financial losses
  - Recovery test verifies the system can restore accurate data and functionality

Appendix K Highlights
Developing the Initial Cyber T&E Strategy (and Updates)

- System description
- System threat assessment
- Systems engineering requirements
- Previous testing
- T&E management
  - CyWG
- Evaluation framework using the Integrated Decision Support Key (IDSK)
  - Data informed decisions – CyWG priorities aligned to leadership decisions
- Cyber DT&E strategy
  - Who, what, where, why, when, how
  - Iterative planning, preparing, executing, evaluating, and reporting
- Resources
  - Contractor and government resourcing

Critical Takeaway and Tailoring

Continuous Planning is the Cornerstone to Cyber DT&E

Image Source: https://www.flickr.com/photos/x1brett/51646283326/in/photostream/

→But *my* program/effort is different/special/fast←

Image Source: https://commons.wikimedia.org/

Section 8 delves into non-acquisition and pre-acquisition, Adaptive Acquisition Pathway considerations, and strategies for tackling challenges in the cyber DT&E process

Section 8 also leans into digital and model-based systems engineering

Streamlining with Digital Engineering (Section 8)

- Digital Engineering enables
  - Earlier discovery
  - Faster iterations for the continuum enabling data informed decisions
  - Efficient resource allocation
  - Improved, consistent data analysis
- Digital twins in cyber DT&E
- Modeling and simulation (M&S) in cyber DT&E
  - Model-based systems engineering (MBSE)
  - Simulations
- Cyber analytic tools to support CyWGs
  - 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
- Leveraging ontologies for enhanced cyber DT&E in MBSE and digital engineering

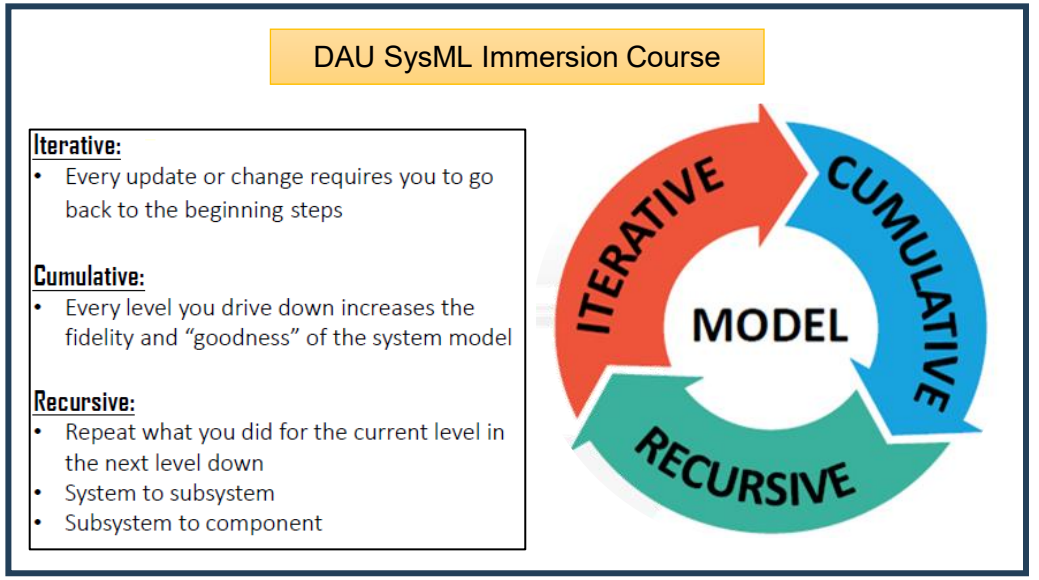


Image Source: Defense Acquisition University

Example EES System Developer M&S Strategy

- Create a high-fidelity system model in SysML
  - Represent the EM1 GWs, EM1 RTs, and the cellular to CIVIL communication network
  - Model the behavior of these components, not just their structure
- Simulate the malicious actor disabling the EM1 GW's navigation data feed
  - This isn't running the actual software; it's running a mathematical representation of the system's behavior
- Verify if the model behaves as expected based on requirements
- MBSE tools allow for behavioral analysis (e.g., state machine diagrams, sequence diagrams) to identify potential bottlenecks or unexpected interactions

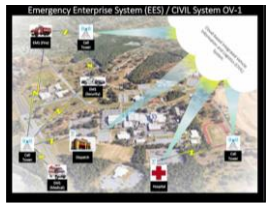


Image Source: 48th Cyberspace Test Squadron

CyWG Ongoing Activities

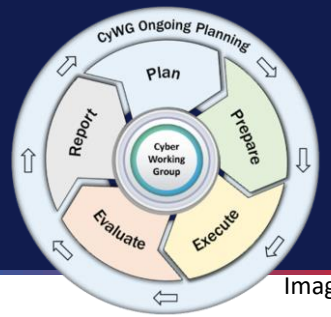


Image Source: DoD Cyber DT&E Guidebook

- Review test environment, processes, and tools
- Analyze existing or known vulnerabilities
- Review contractor test plans as received
- Leverage all available and relevant test data for test planning
- Conduct test readiness reviews
- Execute government acceptance cyber T&E, government cyber DT&E, or integrated cyber developmental and operational tests
  - Independent evaluations
  - Regression test events
- Review cyber test results, plans for remediation and regression testing, and recommend mitigation strategies
- Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones for Authorizing Official review
- Report and track cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users
- Develop strategy and frequency for sustainment cyber DT&E activities

Microcosm within Larger, Integrated Context –
Contracts, System Security Engineering, T&E Responsibilities and Regular Leadership Reviews

Cyber DT&E in the Software Pathway

(1) Planning. (2) Execution Pre-Minimum Viable Capability Release (MVCR). (3) Execution MVCR.

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3
Establish and charter the CyWG	●		
Examine and advise on cyber requirements	●	●	●
Examine threat assessments and characterize attack surface	●	●	●
Support criticality and MRT-C analysis	●	↻	↻
Conduct or update MBCRA	●	○	○
Develop or update cyber DT&E strategy	●	↻	↻
Determine test infrastructure, tools, and data requirements	●	↻	↻
Plan resources and schedule government DT&E	●	↻	↻
Include cyber DT&E requirements in each RFP and contract	●	○	○
Review system developer (contractor) or government development and test environment, processes, and tools	●	↻	↻
Analyze existing or known vulnerabilities		●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received		●	●
Leverage all available and relevant test data for test planning and ensure all test data is made available for subsequent testing		●	●
Conduct test readiness reviews		●	●
Execute security verification throughout the system's life cycle		●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system		●	●
Execute planned government acceptance cyber T&E		●	○
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events		●	●
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies		●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01		●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●
Plan and update sustainment cyber DT&E activities and frequency	●	↻	↻

Image Source: DoDM 5000.UY. Page 46

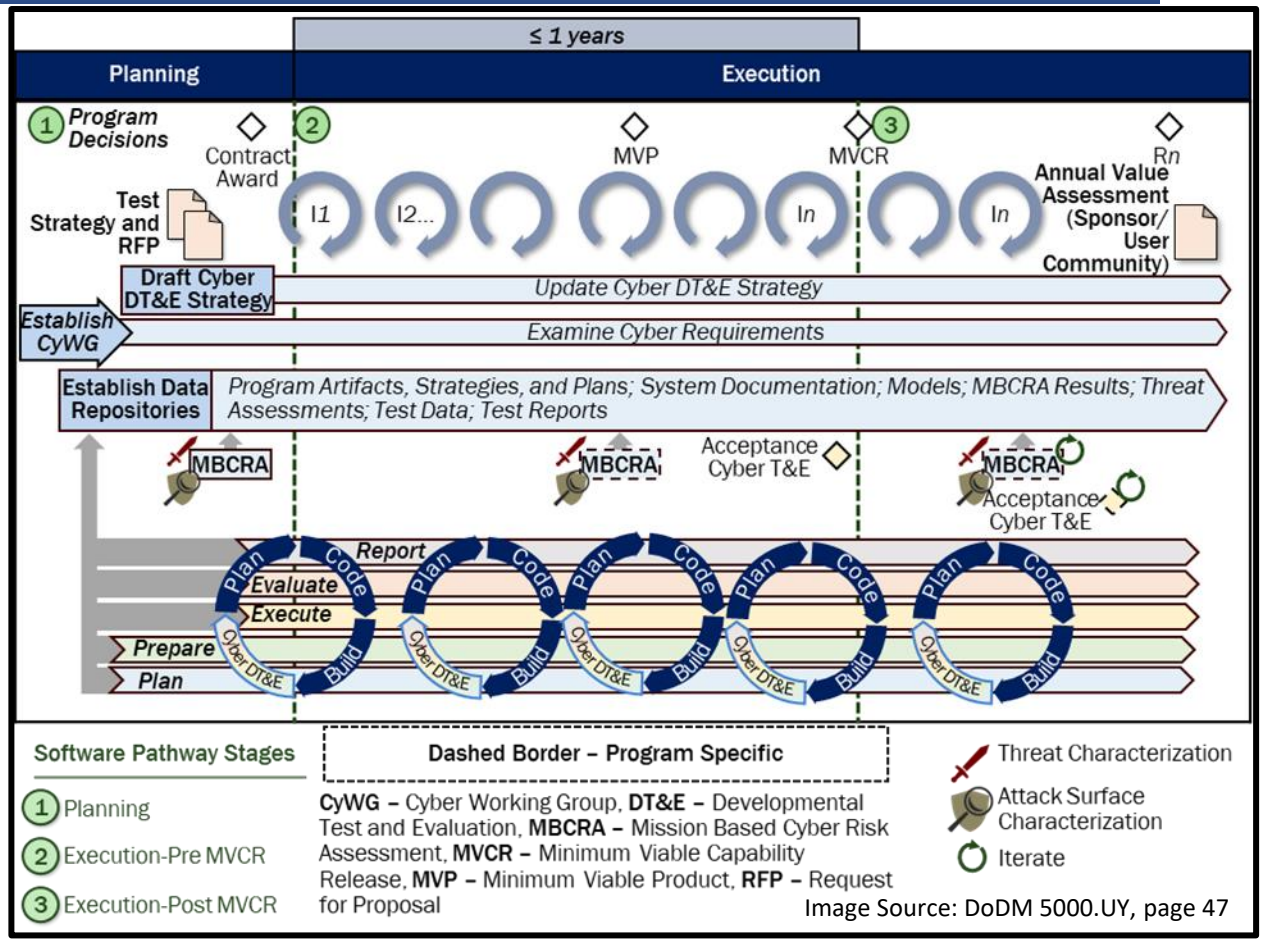


Image Source: DoDM 5000.UY, page 47

In Stage 3, the program sets the pace for required activities.

Summary

- Assessing cyber resilience requires systems engineering and iterative test-fix-test
  - Requirements decomposed and allocated to system levels with measurable and testable criteria
    - Enables tradeoff and comprehensive understanding of system capabilities in mission context
  - Some (non measurable or testable) requirements may need to be verified through demonstration, examination, or analysis (minimize these)
  - Continuously assess changes to cyber risks stemming from software updates, system modifications, evolving threats, and new technologies

- Every system *is* a snowflake and cookie cutter approaches are ineffective
  - Start early with a CyWG and MBCRA – **MISSION CONTEXT MATTERS**
  - Use continuous planning to scope and find repeatable methods to conduct test and assess resilience throughout life cycle – campaign of learning driving data-informed decisions
  - Communicate with others to share best practices and data!

Use the Cyber DT&E Guidebook V3 to help plan the DT&E

Image Source: https://www.qr-code-generator.com/

Questions

DTE&A Cyber

OSDRE-DTEA-Cyber@groups.mail.mil

https://www.cto.mil/dtea/cyber/

Images Source: Microsoft