



Cybersecurity Test and Evaluation Overview

May 4, 2015

Dave Aland
DOT&E

Terry Murphy
DASD(DT&E)

Cleared for open publication
May 14, 2015
DoD Security Review

UNCLASSIFIED



Purpose

Provide a Cybersecurity T&E overview

Cybersecurity T&E closes the gaps between policy, process and execution



Agenda

- **Setting the Stage**
 - DoD Cyber Strategy
 - Policy
- **Cybersecurity T&E overview**
 - Implementation Guidance

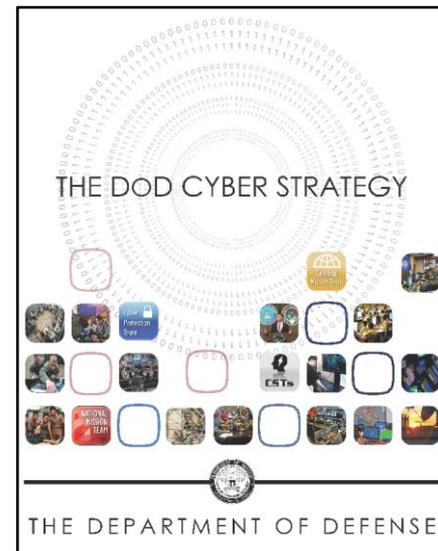


The DoD Cyber Strategy

“We are vulnerable in this wired world”

- **“Today our reliance on the confidentiality, availability, and integrity of data stands in stark contrast to the inadequacy of our cybersecurity”**
- **“The focus is on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information and to defend the nation against cyberattacks”**
- **Three Primary Missions in Cyberspace**
 1. DoD must defend its own networks, systems, and information.
 2. DoD must be prepared to defend the United States and its interest against cyber attacks.
 3. DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

The DoD
Cyber Strategy



Source: The DoD Cyber Strategy, April 2015



The DoD Cyber Strategy

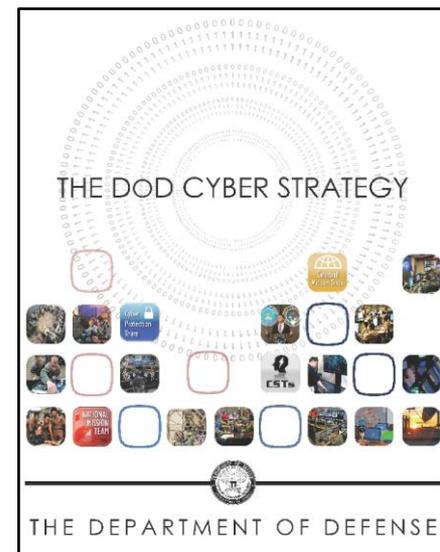
- **DoD sets five strategic goals for its cyberspace missions**

1. Build and maintain ready forces and capabilities to conduct cyberspace operations
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages
5. Build and maintain international alliances and partnerships to deter shared threats and increase international security and stability

- **Key to acquisition is strategic goal 2:**

1. Strengthen DoD's procurement and acquisition cybersecurity standards
2. Mitigate known vulnerabilities
3. Improve the effectiveness of the current DoD Computer Network Defense Service Provider (CNDSP) construct in defending and protecting DoD networks
4. Plan for network defense and resilience
5. Red team DoD's network defense
6. Improve accountability and responsibility for protection of data across DoD and the Defense Industrial Base

The DoD Cyber Strategy



Source: The DoD Cyber Strategy, April 2015



Policy

- DoDI 5000.02, Operation of the Defense Acquisition System
- DoDI 8500.01, Cybersecurity
- DoDI 8510.01, Risk Management Framework (RMF)

DoDI 5000.02

 Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System
References: See References

1. **PURPOSE** This instruction:

- a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), revises the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (e).
- b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

2. **APPLICABILITY** This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Component").

3. **POLICY** The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. **RESPONSIBILITIES**

- a. **Defense Acquisition Executive (DAE)** The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may

DoDI 8500.01

 Department of Defense
INSTRUCTION

NUMBER 8500.01
March 14, 2014
DoD CIO

SUBJECT: Cybersecurity
References: See Enclosure 1

1. **PURPOSE** This instruction:

- a. Revises and restores DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.01 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
- b. Incorporates and cancels DoDI 8500.01 (Reference (c)), DoDD C-5300.10 (Reference (d)), DoDI 8533.01 (Reference (e)), Assistant Secretary of Defense for Networks and Information Integration (ASD/NII)/DoD Chief Information Officer (DoD CIO) Memorandums (References (f) through (h)), and Directive-type Memorandum (DTM) 08-000 (Reference (i)).
- c. Establishes the positions of DoD principal authorizing official (PAO) (formerly known as principal accounting authority) and the DoD Senior Information Security Officer (SISO) (formerly known as the Senior Information Assurance Officer) and continues the DoD Information Security Risk Management Committee (DoD IRMCM) (formerly known as the Defense Information Systems Network (DISN) Global Information Cost (GIC) Flag Panel).
- d. Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (a)) to be used throughout DoD instead of the term "information assurance (IA)."

2. **APPLICABILITY**

- a. This instruction applies to:
 - (1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Component").

DoDI 8510.01

 Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)
References: See Enclosure 1

1. **PURPOSE** This instruction:

- a. Revises and restores DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).
- b. Implements Reference (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).
- c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.
- d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.
- e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD and between DoD and other federal agencies, for the authorization and connection of information systems (IS).

2. **APPLICABILITY**

- a. This instruction applies to:
 - (1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and



DoDI 5000.02

- **T&E Activities**

- Support cybersecurity assessments and authorization
- Provide data to the Program Manager (PM) to enable root cause determination and to identify corrective actions

- **T&E Planning Considerations**

- Develop a strategy and budget resources for cybersecurity testing. The test program will include, as much as possible, activities to test and evaluate a system in a mission environment with a representative cyber-threat capability.
- TEMP at Milestone A
 - “The evaluation methodology will support a Milestone B assessment of planning, schedule and resources and a Milestone C assessment of performance, reliability, interoperability, and cybersecurity.”
- To emulate hostile penetration of information systems, ensure threat appropriate testing is planned and resourced (and occurs in relevant operational environments)
- Security controls implemented consistent with system classification

- **T&E Reports**

- Include Cybersecurity within the Milestone C DT&E Program Assessment
- Integrate the Risk Management Framework (RMF) with T&E
- RMF steps and activities should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation



DoDI 8500.01 / DoDI 8510.01

- **DoDI 8500.01, Cybersecurity**

- DASD(DT&E) and DOT&E collaborate on development of procedures for cybersecurity T&E
- Coordinate with the Test Resource Management Center (TRMC) for establishment of DT&E specific cybersecurity test architectures and requirements
- DOT&E, programs perform cybersecurity assessments as part of operational test assessments.
- DoD Component:
 - Provides for cybersecurity testing capability
 - Conducts vulnerability assessments
 - Ensures cybersecurity T&E is conducted throughout the acquisition lifecycle

- **DoDI 8510.01, Risk Management Framework (RMF)**

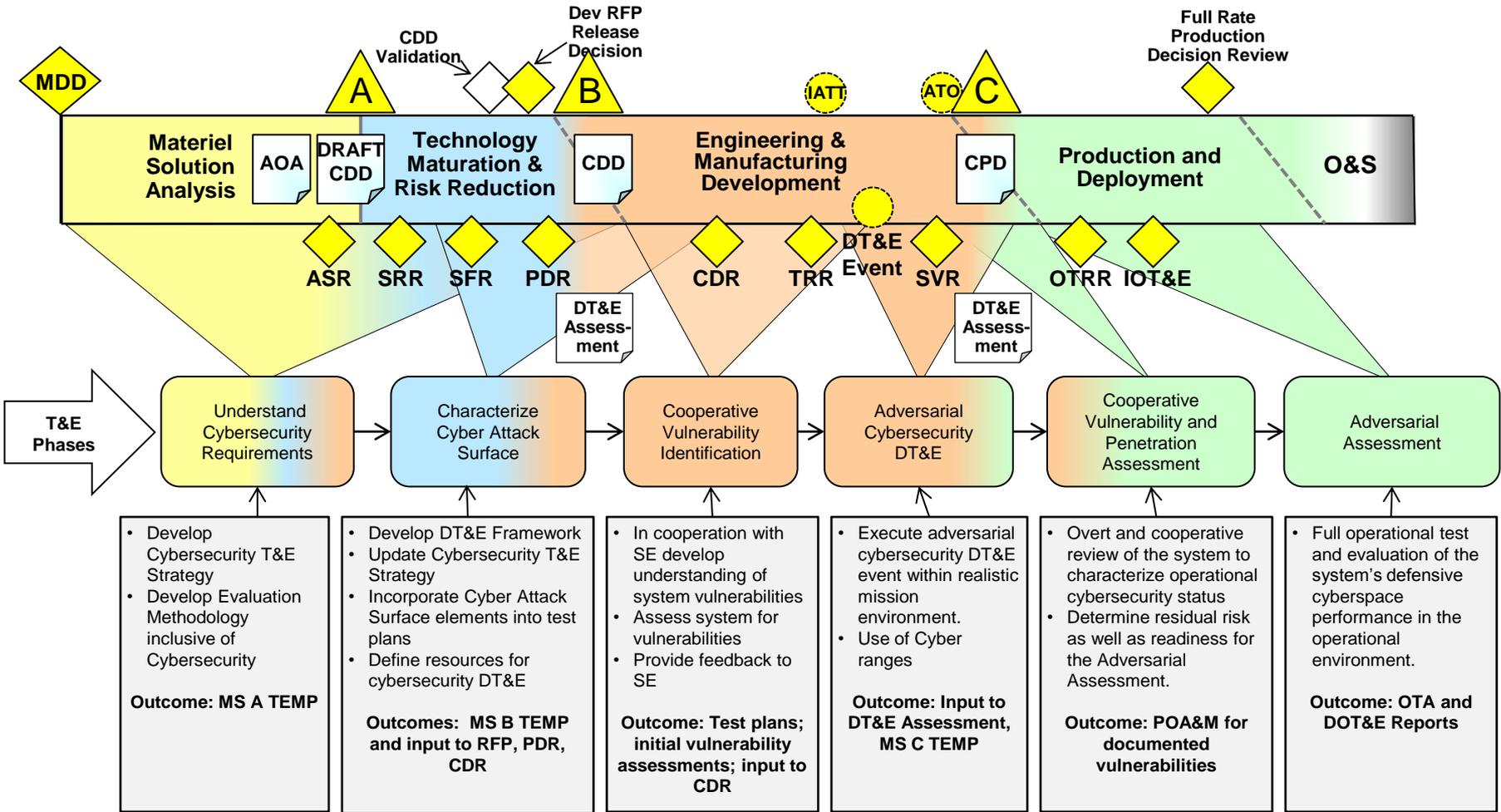
- The RMF process will inform the acquisition process for all DoD Information Technology (IT), including developmental and operational T&E
- Ensure T&E of the assigned Information System (IS) and IT system is planned, resourced, and documented in the program T&E Master Plan (TEMP)



CYBERSECURITY T&E OVERVIEW



Cybersecurity T&E Process



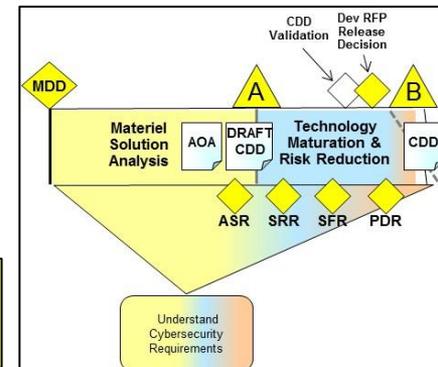
Phases are iterative and executed as part of the Acquisition continuum.



Phase 1 – Understand Cybersecurity Requirements

Understand the program's cybersecurity requirements and develop an initial approach and plan for conducting cybersecurity T&E

- Early in the acquisition process, the Chief Developmental Tester and T&E Working Integrated Product Team (T&E WIPT)
 - Identify cybersecurity requirements and ensure they are complete and testable
 - Review cybersecurity requirements in the System Requirements Document, Program Protection Plan (PPP), technical documents, RMF artifacts, and Request for Proposals (RFPs)
 - Review threat documents to understand the cyber threats to the system
- Based on the requirements review, the T&E WIPT constructs a T&E strategy that addresses cybersecurity
- This phase may be performed iteratively, as system development proceeds



The Chief Developmental Tester and T&E WIPT will ensure that system cybersecurity requirements are identified and are testable

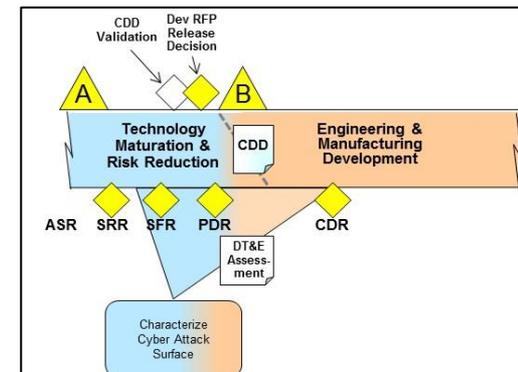


Phase 2 – Characterize Cyberattack Surface

Identify opportunities an attacker may use in order to plan testing to evaluate whether those opportunities continue to allow exploitation

- The attack surface is the system's exposure to reachable and exploitable cyber vulnerabilities, including reliance on supporting / underlying infrastructure
- In collaboration with the systems security engineering process, characterize the cyberattack surface
- RMF artifacts such as the Security Plan and Security Assessment Plan are leveraged to identify additional components that constitute the system's attack surface

Characterization of the cyberattack surface provides input into subsequent test planning



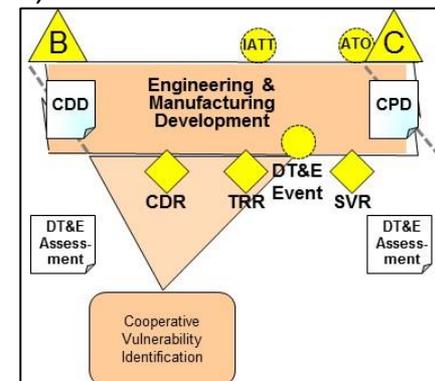


Phase 3 – Cooperative Vulnerability Identification

Analyze and evaluate potential vulnerabilities to determine measures to improve resilience (cyber range or lab)

- Develop initial concept for cyber security testing activities at the component and subsystem level
 - Identify test opportunities to conduct cybersecurity testing in a system of systems context (such as JITC interoperability testing)
 - Identify and integrate RMF security controls assessment activities into unit testing, functional testing, etc.
 - Review early RMF artifacts
- Perform a vulnerability assessment using a Blue Team, to determine likely avenues of cyber attack and the most likely threat exploits
 - Include or emulate the Computer Network Defense Service Provider (CNDSP)
 - Analyze the kill chain
 - Enumerate discovered vulnerabilities
 - Provide feedback to Systems Engineering

Vulnerability testing will be integrated, to the extent possible, with other system test events



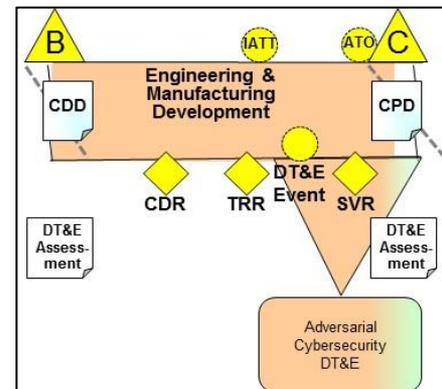


Phase 4 – Adversarial Cybersecurity DT&E

Evaluate the system's cybersecurity in a mission context, using realistic threat exploitation techniques, while in a representative operating environment

- Verify/Exercise Critical Missions through an adversarial, Red Team-type exercise
- Identify exposed vulnerabilities/mission impact
- Develop DT&E Program Assessment, including:
 - How critical mission objectives will be impacted if the data required to execute the mission objectives is altered due to cyberattack and/or exploitation
 - How critical mission objectives will be compromised if required data is unavailable
 - How critical mission objectives will be compromised if mission data is exploited in advance of mission execution

The goal of the cybersecurity DT&E event is to discover critical vulnerabilities and determine their impacts

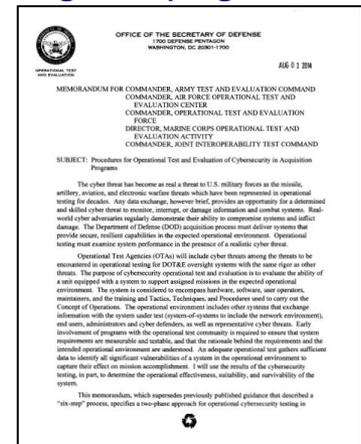




DOT&E Aug 1, 2014 Memorandum

- **New procedures supersede previously issued DOT&E guidance from 2009/2010/2013**
- **Provides a two-phase approach:**
 - Cooperative and comprehensive assessment to identify vulnerabilities (and correct if possible)
 - Threat-representative adversarial assessment for mission effects
- **Provides specific direction on minimum data Operational Test Agencies (OTA) should collect**
 - Supports independent analysis by DOT&E
- **The results of the cybersecurity OT&E will help determine operational effectiveness, suitability, and survivability**

DOT&E Memorandum: Procedures for OT&E of Cybersecurity in Acquisition Programs (August 2014)





What is tested?

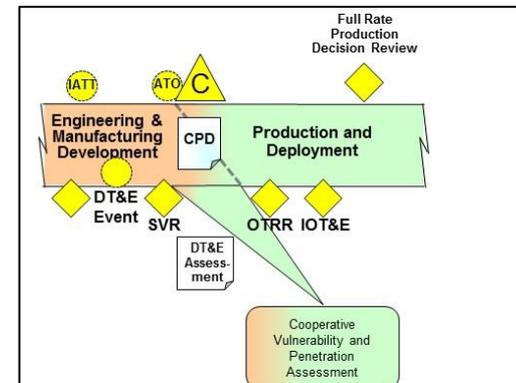
- **All programs on DOT&E oversight that send or receive digital information via:**
 - Direct or indirect connections to external networks
 - Wireless or radio frequency connections
 - Physical ports (e.g. USB), removable data cards
 - Non Internet Protocol-based data buses (e.g. 1553)
- **Any systems with two-way data transfer capabilities to external networks**
- **DOT&E will evaluate the level of test required for other systems on a case-by-case basis**
- **Operational Test Agencies are encouraged to apply the procedures to all information handling systems, regardless of oversight**



Phase 5 – Cooperative Vulnerability and Penetration Assessment

Cooperative operational cybersecurity testing with all stakeholders, including program office, system administrators, and developers

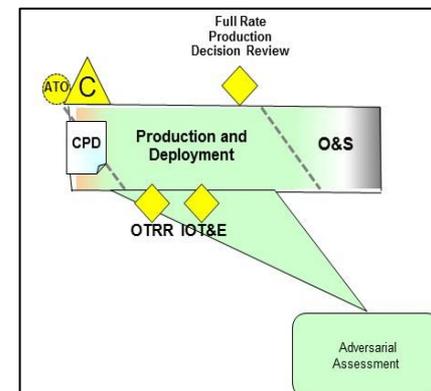
- **Identify all vulnerabilities in as operationally representative context as possible**
 - Introducing systems into the operational environment often adds vulnerabilities
 - Unprotected data paths to networks and other systems
 - Misconfigured cyber defense systems
 - Inadequate physical security
 - Deficient operator Tactics, Techniques, and Procedures
 - But the operational environment also provides defensive capabilities
 - Firewalls
 - Upper-echelon defenses
 - Gateways and enclave boundaries





Phase 6 – Adversarial Assessment

- **Non-cooperative assessment conducted with a threat-representative cyber adversary (Red Team)**
 - Red Team must be National Security Agency (NSA) certified and accredited by U.S. Strategic Command (USSTRATCOM) to operate on live networks, as per Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.03, February 28, 2013
- **Focus is on mission accomplishment, and impact to the mission from vulnerabilities and exploits**
 - Red Team goal is to compromise the system and induce effects
 - The severity of mission effects will inform DOT&E assessment of the impact of cyber vulnerabilities
- **The Operational Test Agency must effectively collect data on Red Team activities, cyber defense activities, and mission effects**
 - System operators should be conducting representative missions
 - Cyber defenders (all echelons) should participate in Operational Testing





Phase 5 & 6 Minimum Data Elements

- **Cooperative Vulnerability and Penetration Assessment**
 - Selected compliance baseline metrics
 - Provide valuable context for other measurements and analysis
 - Cyber vulnerabilities with Defense Information Systems Agency (DISA) severity codes
 - Penetration/exploitation techniques, timing, level of difficulty
 - Password strength
- **Adversarial Assessment**
 - Adversarial activities
 - Times to detect
 - Defense activities
 - System restoration activities
 - Mission effects



Implementation

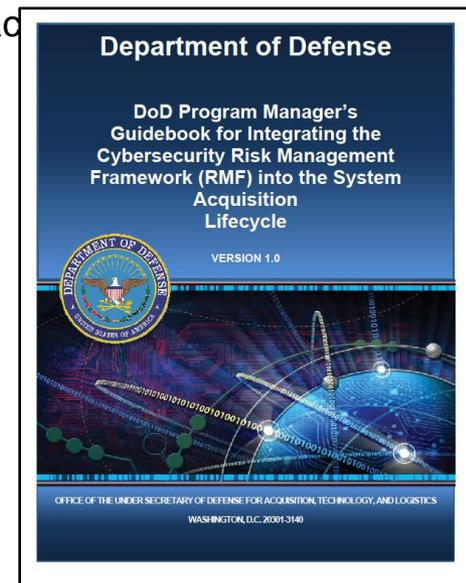
- **Cybersecurity T&E implementing guidance is provided via these documents:**
 - DoD PM's Guidebook for integrating the Cybersecurity Risk Management Framework (RMF) into the Systems Acquisition Lifecycle
 - DAG Chapter 9 (T&E), Paragraph 9.6.5 (Cybersecurity T&E)
 - Cybersecurity T&E Guidebook (expands on DAG Cybersecurity T&E guidance)



DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle

- **DoD Chief Information Officer (CIO) and AT&L co-chair as a collaborative initiative**
- **Purpose - provides cybersecurity integration guidance targeted at the needs of the Program Manager**
 - Provides the Program Manager key areas of consideration during the definition, design, development, assessment and deployment of the system
 - Leverages a multitude of DoD instructions and Federal guidance in order to synthesize into a useable form for Program Managers to apply
 - Offers an approach for the integration of cybersecurity throughout the ac

Approved for release
Anticipate publication in June 2015





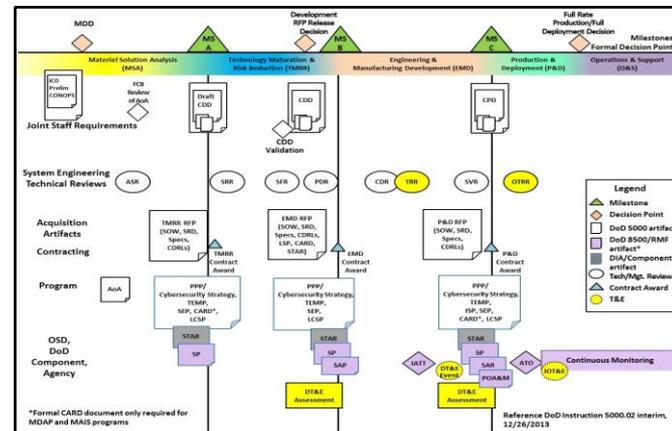
DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle

Table of contents

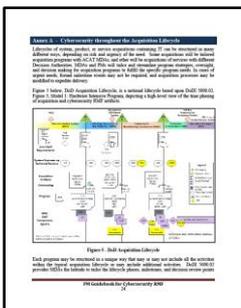
1. Introduction
2. Program Manager Cybersecurity Basics
3. Acquisition Lifecycle Cybersecurity Activities & Process Flow

Annexes

- A. Cybersecurity throughout the Acquisition Lifecycle
- B. Cybersecurity Roles & Responsibilities
- C. Cybersecurity Engineering Considerations
- D. Cybersecurity T&E Considerations
- E. Cybersecurity Lifecycle & Sustainment Considerations
- F. Cybersecurity Risk Assessment Process
- G. Summary of Cybersecurity-Related Artifacts
- H. Cybersecurity RFP Considerations



Annex A



Annex B



Annex C



Annex D





Defense Acquisition Guidebook

- **Section 9.6.5, Cybersecurity T&E**

- **Introduction**

- Cybersecurity threats are dynamic and evolving
- Early Cybersecurity T&E needs to provide timely feedback to Program Manager
- T&E activities need to identify exposed vulnerabilities and provide feedback to Systems Engineering for appropriate mitigation
- T&E activities need to be continuous, iterative, and integrated with current policy

- **Overview of Cybersecurity T&E Phases**

- **References the Cybersecurity T&E Guidebook for additional guidance**

Defense Acquisition Guidebook

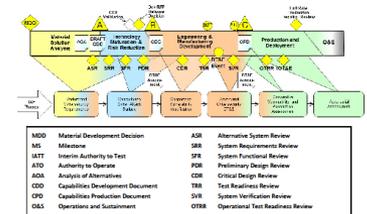
9.6.5. Cybersecurity T&E

DoD missions increasingly depend upon complex, interconnected IT environments. These environments are inherently vulnerable, providing opportunities for adversaries to negatively impact DoD missions. Addressing cybersecurity early in the acquisition process requires a comprehensive T&E program, which provides early discovery and allows for correction of developmental and operational issues, in support of the warfighter.

This section provides an overview to assist the Chief Developmental Testers and the entire test community in developing an approach to cybersecurity T&E. Cybersecurity remains an integral part of developmental and operational T&E. Cybersecurity T&E planning, analysis, and implementation develops an iterative process starting at the beginning of the acquisition lifecycle and continuing through maintenance of the system.

Figure 9.6.5.F.1 depicts the Cybersecurity T&E Process phases, occurring from pre-Milestone A test planning, through developmental test, to cybersecurity OT&E after Milestone C.

Figure 9.6.5.F.1 - Cybersecurity T&E Process Mapped to the Acquisition Lifecycle

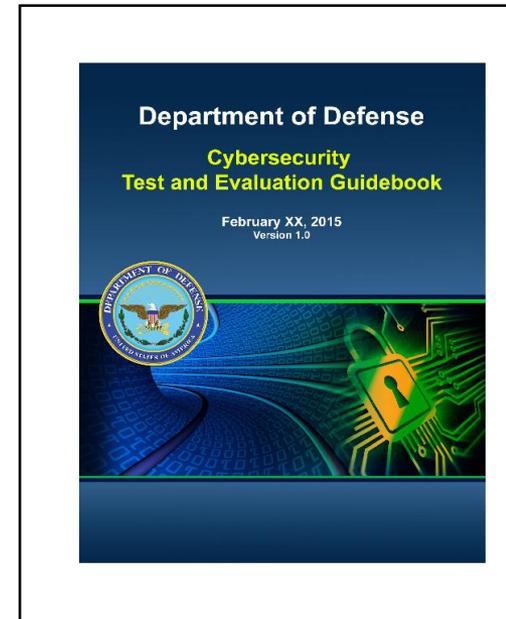




Cybersecurity T&E Guidebook

- **Purpose - provide guidance to assist the Chief Developmental Testers, Operational Test Agencies, and the larger T&E community in developing an approach to cybersecurity T&E**
- **Contents**
 - Introduction
 - Overview of Risk Management Framework
 - Cybersecurity T&E process and implementation guidance
 - Appendixes
 - Analysis Guidance for Risk Management Framework Artifacts
 - DT&E Cybersecurity Issues and Measures
 - OT&E Cybersecurity Issues and Measures
 - Program Protection Plan Analysis Guidance for T&E
 - Cybersecurity T&E Resources
 - Cyber Ranges and Other Facilities
 - Examples of Common Vulnerabilities
 - Primary Stakeholders
 - Glossary and Acronyms

Cybersecurity T&E Guidebook





QUESTIONS?