Department of Defense

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

September 2015

VERSION 1.0

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

WASHINGTON, D.C. 20301-3140

DISTRIBUTION STATEMENT A. Approved for public release.

Cleared for Open Publication

May 26, 2015

DoD Office of Prepublication and Security Review

Executive Summary

Department of Defense (DoD) systems and networks are constantly under cyber attack. Nearly all defense systems incorporate information technology (IT) in some form, and must be resilient from cyber adversaries. This means that cybersecurity[1] applies to weapons systems and platforms; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems; and information systems and networks. Cybersecurity is a critical priority for the DoD, and is a vital aspect of maintaining the United States' technical superiority. DoD recently revised several of its policies to more strongly emphasize the integration of cybersecurity into its acquisition programs to ensure resilient systems. This guidebook is intended to assist Program Managers (PM) in the efficient and cost effective integration of cybersecurity into their systems, in accordance with the updated DoD policies. The guidebook is based on the following DoD policies:

- Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 12, 2014; cancels the previous DoD Information Assurance Certification and Accreditation Process (DIACAP) and institutes a new, risk-based approach to cybersecurity.
- DoDI 8500.01, *Cybersecurity*, March 14, 2014; establishes that cybersecurity must be fully integrated into the system lifecycle.
- DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015; includes regulatory cybersecurity requirements in the following Enclosures: 3 – Systems Engineering (SE), 4 – Developmental Test and Evaluation (DT&E), 5 – Operational and Live Fire Test and Evaluation (OT&E and LFT&E), and 11 - Requirements Applicable to all Programs Containing IT; establishes that cybersecurity 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.

Additionally, the Joint Capabilities Integration and Development System (JCIDS) Manual, updated February 12, 2015, implements a robust cyber survivability requirement within the mandatory system survivability Key Performance Parameter (KPP). This new requirement will enhance system resilience in a cyber-contested environment or after exposure to cyber threats.

The risk management framework (RMF) brings a risk-based approach to the implementation of cybersecurity. Transition to the RMF leverages existing acquisition and systems engineering personnel, processes, and the artifacts developed as part of existing systems security engineering (SSE) activities. Unlike a compliance-based checklist approach, the RMF supports integration of cybersecurity in the systems design process, resulting in a more trustworthy system that can dependably operate in the face of a capable cyber adversary. This guidebook emphasizes integrating cybersecurity activities into existing processes including requirements, SSE, program protection planning, trusted systems and networks analysis, developmental and operational test and evaluation, financial management and cost estimating, and sustainment and disposal.

[1] The revised policies and this guidebook reflect the Department's decision to adopt the term *cybersecurity* in place of *information assurance*.

This guidebook is based on a set of key tenets that form the basis for the guidance that follows. The following tenets are not exhaustive, but do outline some of the more important concepts and principles that should be followed to successfully implement the RMF process into acquisition systems:

- Cybersecurity is risk-based, mission-driven, and addressed early and continually.
- Cybersecurity requirements are treated like other system requirements.
- System security architecture and data flows are developed early, and are continuously updated throughout the system lifecycle as the system and environment (including threats) change, to maintain the desired security posture based on risk assessments and mitigations.
- Cybersecurity is implemented to increase a system's capability to protect, detect, react, and restore, even when under attack from an adversary.
- A modular, open systems approach is used to implement system and security architectures that support the rapid evolution of countermeasures to emerging threats and vulnerabilities.
- Cybersecurity risk assessments are conducted early and often, and integrated with other risk management activities.
- As the system matures and security controls are selected, implemented, assessed, and monitored, the PM collaborates with the authorizing official (AO), the individual responsible for ensuring the cybersecurity risk posture of the system is managed and maintained during operations, to ensure the continued alignment of cybersecurity in the technical baselines, system security architecture, data flows, and design.
- Reciprocity is used where possible through sharing and reuse of test and evaluation products i.e., "test once and use by all."

Comments, suggestions, questions, and proposed changes to this document should be emailed to DoD.PM.Cybersecurity.comments@mail.mil.

Table of Contents

1 Introduction ... 1

1.1 Purpose ... 1

1.2 Applicability ... 2

1.3 Background ... 3

2 PM Cybersecurity Basics ... 5

2.1 General Expectations for Program Managers ... 5

2.1.1 Cybersecurity Basics ... 5

2.1.2 PM Cybersecurity Responsibilities ... 6

2.1.3 ISSM Roles and Responsibilities in Support of the Program Manager ... 8

2.1.4 Cybersecurity Strategy Requirement ... 9

2.2 Functional Activities ... 10

2.2.1 Cybersecurity Requirements Analysis and Definition ... 10

2.2.2 Categorization by Confidentiality, Integrity, and Availability Impact Levels ... 10

2.2.3 Functional Decomposition and Allocation of Cybersecurity Requirements ... 11

2.2.4 Design and Development ... 11

2.2.5 Configuration Management ... 12

2.2.6 Risk Assessment ... 12

2.2.7 Threat Analysis ... 13

2.2.8 Cybersecurity Validation, Test, and Evaluation ... 13

2.2.9 Test Plans and Reports ... 14

2.3 Risk and the RMF Governance Structure ... 15

2.4 Resolving Conflict Arising from Cybersecurity Implementation ... 16

3 Acquisition Lifecycle Cybersecurity Activities and Process Flow ... 18

3.1 Requirements ... 19

3.2 Development ... 19

3.3 Authorization ... 20

3.4 Operations ... 21

Annex A - Cybersecurity Throughout the Acquisition Lifecycle ... 22

A.1 Materiel Solution Analysis (MSA) Phase ... 24

A.1.1 Cybersecurity Assessment Criteria for Analysis of Alternatives (AoA) ... 24

A.1.2 Develop Initial Cybersecurity Strategy and Include Cybersecurity in MS A Documentation 26
A.2 Technology Maturation and Risk Reduction (TMRR) Phase 31
A.2.1 Include Cybersecurity in System Design and Development RFP Release Decision Documentation 31
A.2.2 Include Cybersecurity in Preliminary Design and Final MS B Documentation 32
A.3 Engineering and Manufacturing Development (EMD) Phase 34
A.3.1 Include Cybersecurity in Detailed Final Design 34
A.3.2 Test Cybersecurity Requirements in a Cyber Threat Environment and Assess Cyber Risk to Support Initial Deployment Decision 37
A.4 Production and Deployment Phase and Operations and Support Phase 38
A.4.1 Production and Deployment: Operationally Test Cybersecurity to Support Full or Final Deployment Decision 38
A.4.2 Operations and Support: Monitor Cybersecurity and Risk after Authorization to Operate to Maintain Security Posture until Disposal 40
Annex B - Cybersecurity Roles and Responsibilities 42
Annex C - Cybersecurity Engineering Considerations 70
C.1 Introduction 70
C.2 Background 70
C.3 Roles and Responsibilities 71
C.4 Cybersecurity Engineering References 72
C.5 Program Protection Planning 73
C.6 TSN Analysis 74
C.7 Requirements Traceability and Security Controls 76
C.8 Selecting and Tailoring Security Controls 77
C.9 Engineering Trade Analyses 80
C.10 Systems Engineering Technical Reviews 81
Annex D - Cybersecurity Test and Evaluation Considerations 82
D.1 Introduction 82
D.2 Cybersecurity Test and Evaluation 83
D.2.1 Developmental Test and Evaluation 83
D.2.1.1 Understand Cybersecurity Requirements 84
D.2.1.2 Characterize the Cyber Attack Surface 84
D.2.1.3 Cooperative Vulnerability Identification 84

D.2.1.4 Adversarial Cybersecurity DT&E 84
D.2.2 Operational Test and Evaluation 85
D.2.2.1 Cooperative Vulnerability and Penetration Assessment 85
D.2.2.2 Adversarial Assessment 85
D.3 Overarching Cybersecurity T&E Guidelines for the PM 85
Annex E - Cybersecurity Lifecycle and Sustainment Considerations 87
Annex F - Cybersecurity Risk Assessment Process 92
F.1 Cybersecurity Risk Assessments 92
Annex G - Summary of Cybersecurity-Related Artifacts 97
Annex H - Cybersecurity Request for Proposal Considerations 104
H.1 Overview 104
H.2 Request for Proposal (RFP) Language 105
H.3 Additional Request for Proposal Information 107
Annex I - Cybersecurity Glossary of Terms and Acronyms 109
Annex J - Training 125
J.1 DoD Risk Management Framework (RMF) Training 125
J.1.1 DISA Training 125
J.1.2 Defense Acquisition University (DAU) Continuous Learning Modules 126
J.1.3 DAU Courses 126
J.2 Other DoD Training Resources 127
J.3 Non-DoD Cybersecurity Training Open to DoD Personnel 127
Annex K - References and Resources 128
K.1 References 128
K.2 Additional Resources 132
K.3 Other Reports, Publications and Products 135
Annex L - Other Cybersecurity Considerations 137
L.1 Risk Management Framework Background Information 137
L.2 Cross Domain Solutions (CDS) Information 139
L.3 Questions Program Managers Can Ask to Determine if Cybersecurity is Integrated into Defense Acquisition Programs 140
L.4 Information Systems and IT Products 142
L.5 Platform Information Technology (PIT) and Platform Information Technology Systems 144

Annex M - Examples of Risk Management Framework (RMF) Implementation 147
M.1 Example 1 — Unmanned Aerial Bomber System (UABS) 147
M.1.1 Introduction 147
M.1.2 Step 1: Categorize System [per Reference (b)]: 148
M.1.3 Risk Management Framework Step 2: Select Security Controls 155
M.1.4 Risk Management Framework Step 3: Implement Security Controls 163
M.1.5 Risk Management Framework Step 4: Assess Security Controls 165
M.1.6 Risk Management Framework Step 5: Authorize Information System 173
M.1.7 Risk Management Framework Step 6: Monitor Security Controls 176
M.2 Example 2 – Practical Automobile Example 180
M.2.1 The Requirement 180
M.2.2 Material Solution Analysis Phase 180
M.2.3 Technology Maturation and Risk Reduction Phase 182
M.2.4 Engineering and Manufacturing Development Phase 183
M.2.5 Production and Deployment 186

Table of Figures

Figure 1. RMF Process 4
Figure 3. Conflict Resolution 17
Figure 4. Acquisition Lifecycle High-Level Cybersecurity Process Flow 18
Figure 5. DoD Acquisition Lifecycle 22
Figure 6. MSA Phase of DoD Acquisition Lifecycle 24
Figure 7. Relating Capabilities/Requirements/Specifications and Security Controls 29
Figure 8. TMRR Phase of DoD Acquisition Lifecycle 31
Figure 9. EMD Phase of DoD Acquisition Lifecycle 34
Figure 10. P&D O&S Phases of DoD Acquisition Lifecycle 38
Figure 11. TSN Analysis 75
Figure 12. Traceability of Requirements to Controls 77
Figure 13. Security Control Selection and Tailoring Process 78
Figure 14 - Cybersecurity T&E Process Mapped to the Acquisition Lifecycle 83
Figure 15. Risk Assessment within the Risk Management Process 92
Figure 16. Generic Risk Model with Key Risk Factors 93
Figure 17. Risk Assessment Process 94
Figure 18. PIT and PIT Systems 145
Figure 19. DoD Plan of Action and Milestone 174

Table of Tables

Table 1. Meanings for RASCI Matrix 45
Table 2. Acronyms for RASCI Roles 45
Table 3. RASCI Matrix for the DoD Acquisition Lifecycle 47
Table 4. Security Control Identifiers and Family Names 79
Table 5. Level of Risk Combination of Likelihood and Impact 96
Table 6. Cybersecurity-Related Artifacts 97
Table 7. Terms 109
Table 8. Acronyms 114
Table 9. Relationship between Types of Information Systems and IT Products 143
Table 10. DoD Information Systems and PIT Systems (Assess & Authorize) 143
Table 11. Other DoD -IT (Assess Only) 144
Table 12. Examples of PIT Systems and Associated PIT 146
Table 13. Information Type Impact Values 148
Table 14. Applicable Overlays 150
Table 15. Security Control Identifiers and Family Names 151
Table 16. Assumptions 159
Table 17. Applicable CCIs 168
Table 18. Likelihood of Threat Events 172
Table 19. Overall Likelihood and Level of Impact 172

1 Introduction

1.1 Purpose

The goal of this *Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle* document is to help program managers (PM) understand how to integrate cybersecurity into their programs throughout the system lifecycle in accordance with the Risk Management Framework (RMF) and through collaboration with their Authorizing Official (AO), the individual responsible for ensuring the cybersecurity risk posture of the system is managed and maintained during operations. Per DoDI 5000.02 and DoDI 8500.01, building cybersecurity into the system early and throughout the lifecycle is required to enable operational and technical cybersecurity risks to be identified and sufficiently mitigated throughout the acquisition process leading to decreased program costs, shortened schedules, and improved system performance, resilience, and trustworthiness.

PMs need to be aware of steps they can take to identify, evaluate, and affordably address cybersecurity vulnerabilities based on risk throughout the system lifecycle. Doing so will ensure systems are adequately and affordably protected against external and internal threats and can maintain their mission capabilities in a cyber-contested operational environment. This guidebook synthesizes applicable Department of Defense (DoD) policies with Federal guidance for PMs to apply within their programs. Cybersecurity management support is typically provided to PMs from their Program Executive Office (PEO) staff. Other external personnel with cybersecurity responsibilities are assigned by the Service/Agency in which the PM resides.

This guidebook describes an approach to integrate key cybersecurity activities during all phases of the system lifecycle, including the definition, design, development, assessment, deployment, operation, maintenance, and disposal of the system. These activities include identifying, assessing, monitoring, and mitigating cybersecurity risks to an acceptable level for systems and the missions they support. PMs need to ensure cybersecurity risks are actively managed consistent with system performance requirements, and are acceptable to the Service-designated AOs, who provide the system Authorization to Operate (ATO). Close coordination between the PM and AO is critical to the management of cybersecurity risks throughout the entire acquisition process. The failure to do so early in the system lifecycle impacts the AO's authorization decision as well as system performance, and program cost and schedule. Without the ATO, a system cannot be operated. PMs should work with their AO to discuss the impact of trade decisions and to reach agreement on the tailored documentation required to support the AO's authorization decision.

The guidebook is organized to provide PMs an understanding of the changes that DoD has implemented in policy to build robust cybersecurity into acquisition programs.

- Section 1 contains background information on recent cybersecurity and acquisition policy changes and information about the applicability of this document.
- Section 2 contains expectations for PMs concerning cybersecurity, including general expectations, some key functional activities that the PM needs to understand, a brief

description of the RMF governance structure, and information for PMs on how to resolve and escalate issues related to cybersecurity conflicts.

- Section 3 describes a high-level process flow of building cybersecurity into programs throughout the acquisition lifecycle.

Annex A examines each phase of the acquisition lifecycle, and highlights cybersecurity-related activities and products in more detail than presented in Sections 2 and 3. Annex B describes cybersecurity-related roles and responsibilities associated with the cybersecurity activities at each phase in the lifecycle and provides a detailed matrix of typical cybersecurity activities and the corresponding stakeholders that are responsible, accountable, supportive, consulted, and/or informed for or by each activity.

Additional annexes provide detailed information for specific cybersecurity-related acquisition considerations, including: engineering, test and evaluation, sustainment, the risk assessment process, sample Request for Proposal (RFP) language for cybersecurity, training, resources, and examples of RMF implementation.

1.2 Applicability

This guidebook is applicable to all acquisitions containing information technology (IT),[2] including programs at all stages in the lifecycle and all acquisition categories. The RMF applies not only to information systems (e.g., computer networks/enclaves and major applications/defense business systems (DBSs)) but to all IT, which includes information systems, weapons systems, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, other platform IT (PIT) systems[3] and PIT (e.g., embedded IT, test and diagnostic equipment, mission planning and support systems, and any other information or IT that connects to or accesses weapons and C4ISR systems). There is no difference in the application of the RMF to DBS information systems from non-DBS information systems (e.g., National Security Systems). PIT systems must be secured and assessed and authorized just like information systems under the RMF; however, PIT systems do not have to be entered into the DoD IT Portfolio Repository (DITPR) and undergo Federal Information Security Management Act (FISMA) compliance/oversight. Both information systems and PIT systems must be registered at the DoD Component level. While DoD did not accredit PIT systems under DIACAP, DoD now authorizes PIT systems (e.g., ships, missiles, airplanes, tanks/vehicles with IT) in accordance with the RMF, due in large part to the interconnected nature of embedded IT in these systems.

Program managers will structure, tailor, and phase their programs to best reflect their program's specific cybersecurity needs. Therefore, some of the acquisition processes and artifacts discussed in the guidebook may not be required for every program or activity. The intent of this guidebook is not to give a precise set of instructions on how to integrate cybersecurity for all programs, but rather to help PMs and their staffs understand the policies, requirements, constraints, and relationships to help them integrate cybersecurity within their own program

[2] DoD instructions use the definition for IT from Committee on National Security Systems Instruction (CNSSI) 4009; that definition is included in Annex K.
[3] See Annex L for information on PIT and PIT systems.

activities and throughout the program lifecycle. Detailed RMF and cybersecurity implementation guidance for security practitioners is available on the RMF Knowledge Service at https://rmfks.osd.mil, an online resource that serves as the definitive source for RMF implementation guidance for DoD, a repository for templates and tools, and a collaboration space for the RMF community.

1.3 Background

The DoD is increasingly reliant on information technology (IT) and its interconnections in major weapons, C4ISR, facilities, and information systems. DoD systems that have significant vulnerabilities threaten the confidentiality, integrity, and availability (C-I-A) of critical information and functionality supporting DoD missions, operations, assets, and personnel. Skilled adversaries target DoD systems, networks, users, and interfaces, seeking opportunities to obtain information and disrupt or alter operations. Building robust cybersecurity capabilities into programs is vital to protecting the Department's critical information, networks, and systems, and to enabling mission success. To guide the integration of robust cybersecurity in the acquisition process, the Department has developed and updated several key policies.

The Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L) memorandum, January 7, 2015, accompanying the DoD Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System*, states that successful defense acquisition depends on careful thinking and sound professional judgments about the best acquisition strategy to use for a given product. It emphasizes tailoring of program structures, content, and decision points to the product being acquired and that programs must deal with the increasingly serious problem of designing for, and managing, cybersecurity in programs. It states that DoD must do a better job of protecting our systems and everything associated with them from cyber threats.

In March 2014, the DoD Chief Information Officer (CIO) published two important documents: DoDI 8500.01, *Cybersecurity*, and DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT).* DoDI 8500.01 establishes that the term "cybersecurity"[4] replaces the term "information assurance" within the DoD. DoDI 8510.01 establishes that the RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) as the process to manage the lifecycle cybersecurity risk to DoD IT.

The RMF transitions DoD from a historically compliance-based process to a risk-based, full-lifecycle approach. DoD cybersecurity policy as implemented through the RMF process is based on the application of security controls, the selection and implementation of which are based on cybersecurity risk assessments and other SSE activities conducted throughout the system lifecycle. A security control is "a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements."[5] Security capability requirements are explicitly defined as part of the system survivability key performance parameter (KPP) and other capability requirements document attributes and are derived as technical requirements in system requirements documents and system and item specifications. PMs are

[4] See the glossary in Annex I for definition of cybersecurity.
[5] *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

encouraged to tailor their cybersecurity approach according to system attributes and to base trade-off design decisions on the System Survivability KPP, other KPPs, and derived cybersecurity requirements of their systems.

The RMF enables the design and integration of cybersecurity early in the system development lifecycle to assist in the development of a trustworthy system that can dependably operate in the face of a capable cyber adversary. Security controls are integrated with system requirements through SSE activities, including applying overlays to the baseline set of controls based on system attributes, system/mission assurance security risk assessments and mitigations, and design trades that factor in cybersecurity along with all other program cost/schedule/performance constraints and risks. Cybersecurity requirements need to be matured and maintained throughout the system lifecycle.

Figure 1 describes the six steps of the RMF process. The following sections describe PM specific activities for implementing these steps and Annex M provides examples of RMF implementation in the acquisition lifecycle.

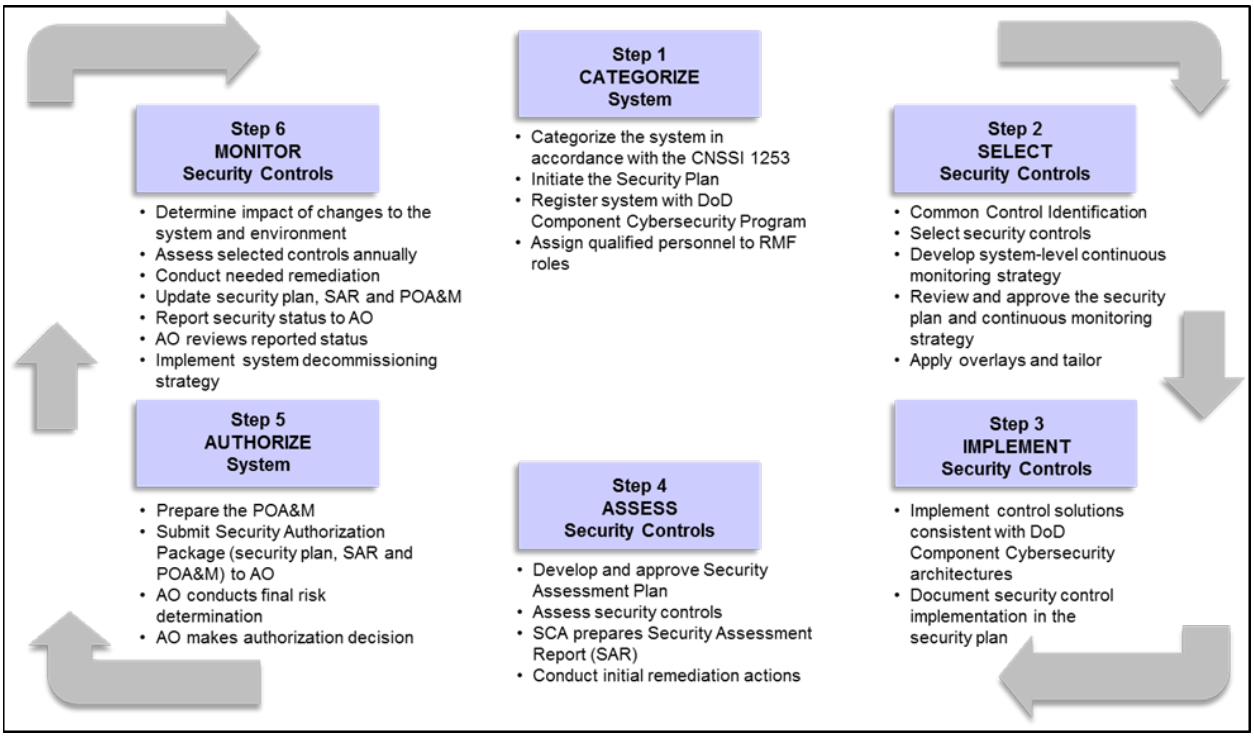


Figure 1. RMF Process

2 PM Cybersecurity Basics

2.1 General Expectations for Program Managers

The PM ensures the program meets statutory, regulatory, and system requirements, balancing lifecycle cost, schedule, system performance, risk, and system security. In doing so, PMs must understand, plan for, and integrate cybersecurity into their programs in a cost-effective manner. PMs need to tightly coordinate requirements generation, systems security engineering, ongoing risk assessments, program protection planning, and test and evaluation. At the same time, PMs need to understand the motivation of adversaries and the system vulnerabilities that may be exploited to disrupt the operation of their systems and the missions their systems enable on the battlefield. PMs must design, develop and produce DoD systems that will be dependable in the face of a sophisticated cyber adversary.

2.1.1 Cybersecurity Basics

The PM is responsible for meeting cybersecurity requirements throughout the lifecycle of the program. DoDI 8500.01, *Cybersecurity*, replaced the term information assurance with cybersecurity and defines cybersecurity as:

> "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"

PMs and Chief Engineers/Lead Systems Engineers who are unfamiliar with the details of the DoD cybersecurity regulations and policies should consider the following three security objectives when trying to balance specific cybersecurity requirements with the other requirements that apply to their system:

- Confidentiality – The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. NIST SP 800.53: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – The property whereby an entity has not been modified in an unauthorized manner. NIST SP 800-53: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability – The property of being accessible and useable upon demand by an authorized entity. NIST 800-53: Ensuring timely and reliable access to and use of information.

It is critical to understand that cybersecurity extends beyond the bounds of information security, to include:

- Solid engineering that includes design features that promote stability and security.
- Training and awareness to provide users, operators, and sustainers with proper training to ensure they are vigilant.

- Response, recovery, and restoration to actively respond to internal and external malicious attacks, as well as recover from system failures caused by inadvertent operator error, internal and external malicious attack, and major calamities.

2.1.2 PM Cybersecurity Responsibilities

Early resourcing and planning is essential to ensure cybersecurity activities, which protect against the full array of applicable external and internal threats, are adequately resourced, executed, and assessed throughout the acquisition lifecycle. While the process assumes that the program is following the guidance provided in DoDI 5000.02 and Defense Acquisition Guidebook (DAG), that does not imply that every system is an acquisition category (ACAT) program (e.g., deployed system in sustainment), or part of an ACAT program. For those systems that are not required to comply with DoDI 5000.02, the Risk Management Framework artifacts (Security Plan, Security Assessment Report (including risk assessment results or separate Risk Assessment Report), and Plan of Action and Milestones (POA&M)) serve as the reporting templates for tracking cybersecurity compliance for the delivered capability. For cybersecurity implementation into acquisition programs, the requirements and acquisition processes can be divided into three sub-processes, each having specific documentation in which cybersecurity should be clearly articulated. These three sub-processes are described in the following sections.

2.1.2.1 Requirements Generation

Requirements generation is described within the Joint Capabilities Integration and Development System (JCIDS). Requirements generation includes the identification of required capabilities, KPPs, key system attributes (KSAs), and additional performance attributes, which are included in the Initial Capabilities Document (ICD), the Capability Development Document (CDD), the Capability Production Document (CPD), the Concept of Operations (CONOPS), the Information Support Plan (ISP), and the Test and Evaluation Master Plan (TEMP). KPPs include the cybersecurity element of the System Survivability KPP and other KPPs as required.

The PM team and requirements developers must be cognizant of the mandatory System Survivability KPP, which includes cyber survivability requirements. The JCIDS Manual, updated on February 12, 2015, requires development of cyber survivability requirements within the System Survivability KPP, if applicable to the operational context. PMs will need to deliver systems that are able to operate and complete their missions in a cyber-contested environment. In practice, this KPP requirement will ensure sponsors devote resources to aid in the development of rigorous cyber survivability analysis and ultimately KPP values, and to ensure minimum cyber survivability-related requirements will be met.

2.1.2.2 Acquisition and Program Management

Acquisition and program management provides oversight of the key acquisition and program management processes and documentation, to include, but not limited to: the Acquisition Strategy (AS); Acquisition Program Baseline (APB); Cybersecurity Strategy; Program Protection Plan (PPP); legacy System Threat Assessment Report (STAR) or other threat source documentation (e.g. Validated Online Lifecycle Threat (VOLT)); Systems Engineering Plan (SEP); Cost Analysis Requirements Descriptions (CARD) for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAISs) only, and rationale for lifecycle cost estimate for other programs; contracts; Requests for Proposal (RFP); Training

Plan; Life Cycle Sustainment Plan (LCSP); Independent Logistics Assessments (ILA) (for weapon system MDAPs only); etc.

PMs must address cybersecurity in program reviews, including Deep Dives, In-Process Reviews, and Overarching Integrated Product Team (OIPT) meetings, Defense Acquisition Executive Summary (DAES) meetings, and Milestone and Decision Point Defense Acquisition Boards/Milestone Decision Authority (MDA) reviews. The PM needs to build an IPT structure that includes cybersecurity expertise. The Program Management Office (PMO) team should work with external stakeholders[6] to build an effective cybersecurity capability. Cybersecurity impacts system and mission performance. For this reason, the PM and acquisition leadership, along with the resource sponsor/capability requirements validation authority, user representative, and the systems engineering (SE) and test communities make cybersecurity trade-offs based on risk and in concert with cost, performance, and schedule constraints. PMs must negotiate risk trade-offs with relevant stakeholders, e.g., AO, Information System Security Manager (ISSM), and others. The PM and AO are the key authorities for most cybersecurity decisions throughout the acquisition lifecycle.

2.1.2.3 Systems Engineering and Test and Evaluation

Implementation of a disciplined systems engineering process that includes cybersecurity is required from requirements analysis through design, test and evaluation, fielding, sustainment, and decommissioning. The cybersecurity design is part of the system's functional design and it is captured in design documentation, such as the System Design Document (SDD)/System Design Specification (SDS)/System Performance Specification (SPS)/System Requirements Document (SRD) and other lower level technical specifications. Cybersecurity will be reviewed along with all technical documentation during prescribed program technical design reviews governed by the System Engineering Technical Review (SETR) processes.

As systems mature throughout implementation and assessment, the PM, in coordination with ISSM and SSE personnel, needs to ensure the continued alignment of cybersecurity requirements in the technical baselines, the system security architecture, information flows, design, and the security controls. The PM needs to coordinate periodically with the AO to maintain awareness of these activities as they affect the security state and risk posture of the system throughout the Production and Deployment and Operations and Support phases. The PMO will develop and implement a continuous monitoring plan to assure the effectiveness of security controls over time, as changes are made to the system and within the operational environment, including the evolving threat. Annex A, section A.4 describes the Production and Deployment and Operations and Support acquisition lifecycle phases and provides more information on the monitoring of security controls.

PMs also need to develop and maintain a PPP and a detailed Cybersecurity Strategy, and utilize them as the program's integrating and central point for cybersecurity. The PM must develop a cybersecurity Test and Evaluation (T&E) strategy, allocate resources for cybersecurity T&E, and ensure they are described in the TEMP. PMs need to consider and integrate cybersecurity, including required resources, in the system's acquisition lifecycle activities including systems

[6] The roles and responsibilities of cybersecurity stakeholders are described in Annex B

security engineering risk assessments, SETRs, cybersecurity T&E, cost estimation, and artifacts including the SEP, TEMP, and RFP.

2.1.3 ISSM Roles and Responsibilities in Support of the Program Manager

The PM is responsible for appointing an Information System Security Manager (ISSM) for each assigned system with the support, authority, and resources to satisfy the responsibilities established in DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT).* In accordance with DoDI 8500.01, *Cybersecurity,* the ISSM needs to be assigned in writing. The PM should ensure that the designated ISSM has the support, authority, and resources to satisfy the responsibilities established in DoDI 8500.01. Assignment of a qualified ISSM is one of the most important steps and should be accomplished as early as possible to ensure that applicable cybersecurity requirements are addressed in the system architecture and detailed design.

DoD Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management*, current edition, provides guidance for the identification and categorization of positions and certifications of personnel conducting cybersecurity functions within the DoD workforce and should be used for selecting an ISSM. As the PM's agent for ensuring compliance with DoD cybersecurity policies and regulations, the ISSM's roles and responsibilities include:

- Ensure compliance with cybersecurity requirements in accordance with DoD and DoD Component cybersecurity and information assurance policies and guidance.
- Support the PM in development of a POA&M and budget that addresses the implementation of cybersecurity requirements throughout the lifecycle of the system.
- Identify a cybersecurity team; the PM can designate the ISSM to chair a Cybersecurity (may be called Information Assurance) Working-level Integrated Product Team (WIPT) or sub-WIPT, executed under the authority of the Systems Engineering WIPT.
- Support implementation of the RMF.
- Maintain and report systems assessment and authorization status and issues in accordance with DoD Component guidance.
- Provide direction to the Information System Security Officer (ISSO) in accordance with DoDI 8500.01.
- Coordinate with the organization's security manager to ensure issues affecting the organization's overall security are addressed appropriately.
- Continuously monitor the system or information environment for security-relevant events and configuration changes that negatively affect security posture.
- Periodically assesses the quality of security controls implementation against performance indicators, such as: security incidents; feedback from external inspection agencies, e.g., Office of the Inspector General (OIG) DoD, Government Accountability Office (GAO); exercises; and operational evaluations, including Director, OT&E cybersecurity assessments.
- Immediately report any significant change in the security posture of the system, and recommended mitigations, to the Security Control Assessor (SCA) and AO.
- Recommend to the SCA or AO a reassessment of any or all security controls at any time, as appropriate.

- Ensure that SSE processes are aligned to, and adequately documented in the program's SEP and PPP, and are executed with sufficient rigor to ensure required security controls are implemented, resulting in the lowest level of residual risk to system operation.
- Ensure that cybersecurity inputs to program acquisition documents are prepared.
- Ensure that the program's contractual documents, such as specifications, statements of work, or Contract Data Requirements Lists (CDRLs) incorporate appropriate cybersecurity language and requirements.
- Support SETRs by ensuring that entry and exit criteria include cybersecurity and are satisfied, and that design documentation meets the specified cybersecurity requirements.
- Ensure that security controls and requirements are properly allocated and documented in design specifications, technical publications and manuals, etc.
- Ensure security controls and requirements are properly allocated and implemented in logistics or program planning documents.
- Ensure that security controls and requirements have been communicated and appropriately resourced by program budget documents and are reflected in the program's requirements database.
- Ensure that integrated logistics support documentation (e.g., LCSP) incorporate cybersecurity considerations throughout the lifecycle of the system.

2.1.4 Cybersecurity Strategy Requirement

Under the Clinger-Cohen Act, a Cybersecurity Strategy is a statutory requirement for mission critical or mission essential IT systems. Per Table 2, page 51, of DoDI 5000.02, the Cybersecurity Strategy is a regulatory requirement for all acquisitions of systems containing IT, including National Security Systems (NSS), PIT, and PIT systems. It is an iterative document that reflects both the program's long-term approach for, as well as its implementation of, cybersecurity throughout the program lifecycle. The Cybersecurity Strategy should be used as a tool for PMs, AOs, cybersecurity, and acquisition oversight authorities to plan for, document, assess, mitigate, and manage risks as the program matures. The PM updates and maintains the Cybersecurity Strategy and ensures it matures with the system design throughout the system lifecycle. The Cybersecurity Strategy consolidates elements of various program initiatives and activities relating to cybersecurity planning guidance and efforts. The reuse of existing analysis and documentation is strongly encouraged where practical for the development of the Cybersecurity Strategy to reduce duplication of content and effort. It is incumbent on the submitting Program Management Office (PMO) to ensure that any such information is readily available to the document review/approval chain by providing copies of any supporting documents upon request, including acquisition baselines, systems engineering analyses, test and evaluation, and RMF documentation.

The Cybersecurity Strategy is used by the AO, and reviewed and approved by the Cognizant Chief Information Officer (CIO) prior to milestones and decisions points. For ACAT I programs, the DoD CIO reviews and approves it. The Cybersecurity Strategy elaborates on the approach and cybersecurity risks and countermeasures employed on the system. Additional information, including the prescribed template and authoritative guidance can be found on the Defense Acquisition Guidebook and the RMF Knowledge Service.

2.2 Functional Activities

2.2.1 Cybersecurity Requirements Analysis and Definition

DoD and DoD Component policy requires all programs to implement cybersecurity. All programs should start with the baseline set of security controls based on the system categorization. There are a number of factors that impact the selection of a system's high-level cybersecurity requirements:

- Results of cybersecurity threat analysis for the system under development.
- Potential impact values for the information types processed, stored, transmitted, or protected by the system; and for the system as they relate to confidentiality, integrity, and availability.
- Functional decomposition and allocation of security controls delineated in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (also called the security control catalog), to the system security architecture (also referred to as the solution architecture) for the system, including all system access points and connections.
- The mission the system is supporting.
- System design features (KPPs, KSAs, and additional performance attributes) that promote stability and security.
- Operating environment (including threat) of the system under development.
- Operational and procedural solutions that may mitigate threats to the system.

The government retains the responsibility and authority for identifying, selecting, and approving the appropriate cybersecurity requirements for consideration in the system design; however, industry expertise may be called upon to evaluate the many factors impacting the cybersecurity design, and to make recommendations as to which cybersecurity requirements should be incorporated into the design of the system. To ensure cybersecurity requirements are considered in the functional design of the system, contracts, Statements of Work, and RFPs need to delineate specific tasks and deliverables in support of cybersecurity. Once the high-level cybersecurity capability requirements have been identified, they should be included in the Draft CDD, CDD, and CPD. In parallel, the requirements should be captured in the program's requirements management database, e.g., Dynamic Object Oriented Requirements System (DOORS) that permits development of a requirements traceability matrix (RTM).

2.2.2 Categorization by Confidentiality, Integrity, and Availability Impact Levels

The determination of system categorization impact levels for the confidentiality, integrity, and availability security objectives is described in Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*. System categorization by C-I-A replaced the use of Mission Assurance Category (MAC) and Confidentiality Level (CL), used under DIACAP. The system categorization drives the baseline set of security controls from CNSSI 1253. DoD uses CNSSI security control baselines for all systems (NSSs and non-NSSs). There are three security objectives and each has three possible values (Low, Moderate, or High). Refer to the RMF Knowledge Service at https://rmfks.osd.mil for more information on security control baselines.

2.2.3 Functional Decomposition and Allocation of Cybersecurity Requirements

The security controls, KPPs, KSAs, and additional performance attributes, including cybersecurity design features, will be functionally decomposed and allocated to various elements within the system, consistent with system security architecture, e.g., the solution architecture. Even if a cybersecurity requirement will be inherited from an enterprise system, it still needs to be documented in the requirements database so that the program RTM accurately reflects the cybersecurity requirements flow down from the system security architecture to the system under development. The program RTM also needs to consider any access points and interconnections, as interconnections to these mission planning and support systems/devices (e.g., test and diagnostic equipment), may impose cybersecurity requirements on the system.

In addition to the elements normally found in the RTM, cybersecurity unique tracking elements should be maintained within the RTM. These cybersecurity unique elements will support development of RMF artifacts, if needed. It is important to note that the cybersecurity elements in the RTM should not be treated as a separate set of requirements, but rather a subset of the program's RTM. The ISSM should exercise caution to ensure that the cybersecurity subset of the RTM is always generated from the program's RTM. Cybersecurity requirements should be updated using a single, authoritative requirements database that is under strict configuration management.

The program ISSM and SSE need to provide rationale for all cybersecurity requirements that cannot be met or are identified as not applicable.

2.2.4 Design and Development

Systems engineers need to ensure that functional design considerations integrate cybersecurity functional requirements and that these requirements are included throughout the development process. The SETR process requires entrance and exit criteria for each design review. Cybersecurity-specific criteria are a subset of the entrance and exit criteria. The design review chairperson validates that the cybersecurity technical requirements are included in design documentation and that all entrance and exit criteria, including the subset of entrance and exit criteria for cybersecurity, are satisfied. System trades consider and prioritize cybersecurity requirements against all other system design requirements. Technical requirements that cannot be met, including cybersecurity requirements, should be assessed for the risk to the program, risk to the performance of the system, and risk to the mission. Risk assessments should be conducted and the results brought to the attention of the PM, Resource Sponsor (also called the Mission Owner), and user representative.

Commercial-off-the-shelf (COTS) cybersecurity products and cybersecurity-enabled products should be certified compliant with Committee on National Security Systems Policy 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, June 2013, as amended, by laboratories accredited under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). Similarly, government-off-the-shelf (GOTS) cybersecurity products or cybersecurity-enabled products the system

employs should be evaluated by the National Security Agency (NSA) or in accordance with NSA approved processes.

2.2.5 Configuration Management

Configuration management is critical to ensuring a successful system design and development process. Controlling and documenting changes in design throughout the analysis, development, and testing process requires strict adherence to an established configuration management process. The configuration management process needs to include changes made to the cybersecurity configuration and associated documentation. Failure to include cybersecurity considerations in the configuration management and engineering change control processes could adversely affect the program's ability to integrate and maintain cybersecurity in the functional design of the system.

2.2.6 Risk Assessment

PMs are responsible for managing risk in accordance with the mandatory requirements contained in the DoDI 5000.02, *Operation of the Defense Acquisition System*, and are required to outline their risk management strategy in accordance with the SEP Outline (2011).

Paragraph 6.d. of Enclosure 2 to DoDI 5000.02, discusses program risk: "The Program Manager is responsible for implementing effective risk management and tracking to include the identification of all known risks, key assumptions, probability of occurrence, consequences of occurrence (in terms of cost, schedule, and performance) if not mitigated, analysis of mitigation options, decisions about actions to mitigate risk, and execution of those actions." *DoD Risk Management Guide for Defense Acquisition Programs*, 7th Edition (Interim Release), December 2014, provides risk management guidance for PMs. The following paragraphs describe how a program performs cybersecurity risk assessments for the system security architecture, including all system access points and connections. The analysis of cybersecurity risks, in addition to supporting the cybersecurity program, supports the program's risk management process, and is utilized in the SETRs.

Cybersecurity risk assessment is the process of identifying, analyzing, and assessing system performance and mission consequences of cybersecurity risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur. A risk model identifies risk factors. The risk factors of concern are threat sources, threat events, likelihood, vulnerabilities predisposing conditions, and impact.

The ISSM and SSE provide the subject matter expertise to plan and execute cybersecurity risk assessment and structured testing that demonstrates satisfaction of cybersecurity requirements. Per the RMF, selection/tailoring of security controls is a risk- and mission-based process to inform requirements, architecture, design, implementation, integration, test and evaluation, and sustainment. The selection, tailoring and implementation of security controls are enabled by the Chief Engineer/Lead Systems Engineer, SSE, ISSM, and Mission Owner. The Program Protection Trusted Systems and Networks (TSN) analysis or another mission-focused risk assessment process consistent with NIST SP 800-30 (Information Security), Revision 1, *Guide*

for Conducting Risk Assessments, are resources available to guide the cybersecurity risk assessments. These security risk functions will be executed using established methods, procedures, and industry best practices. The ISSM and SSE need to communicate the status of technical cybersecurity risk assessments to the PM as new risks are identified and old risks are retired.

A more detailed discussion of technical cybersecurity risk assessment is provided in Annex F, Cybersecurity Risk Assessment Process. Also see Annex C, sections C.5 and C.6, for more information on trusted systems and networks analysis, cybersecurity engineering considerations, criticality analysis, threat assessment, vulnerability assessment, risk assessment, and countermeasure selection and application.

2.2.7 Threat Analysis

For cybersecurity, a "threat" is defined as a tool, technique, or methodology with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. A cybersecurity threat analysis results in a list of actors, tools, techniques, and methodologies that can be used to target the system under development.

The intelligence analysts performing the cyber threat analysis do not necessarily reside within the PM office; however, the work is performed on behalf of the PEO from relevant intelligence sources. To apply the cyber threat analysis to a specific system, the engineer should start with a defined list of threats that can be used to attack the system or the information being processed, including methods, tools, and techniques and should add them to the threat information available from authoritative sources such as the Defense Intelligence Agency (DIA), and National Threat Operations Center (NTOC). Each threat should be evaluated for applicability to the system or information being processed, i.e., the evaluation should consider whether the tool, technique, or methodology can be used to attack and exploit system vulnerabilities or the information being processed by the system and the likelihood of such an attack. The finalized list of applicable threats should be included in the overall threat list for the system. The cybersecurity threats to the system should be continually reviewed and updated throughout the lifecycle of the system. This list of applicable threats and system vulnerabilities will be used to support cybersecurity risk assessments as part of the RMF, and will inform mitigation activities.

2.2.8 Cybersecurity Validation, Test, and Evaluation

2.2.8.1 Cybersecurity Validation

In preparation for each technical review, the AO will direct a technical risk assessment of cybersecurity, based on sound engineering judgment and incremental testing to validate implementation of security controls, KPPs, KSAs, and additional performance attributes. Using the completed cybersecurity risk assessment, the AO or the designated representative will validate the cybersecurity design of the system and report those findings to the Milestone Decision Authority, the PEO, and the PM.

2.2.8.2 Integrated, Incremental Cybersecurity Test and Evaluation

Implementation of the RMF does not fully ensure a program is prepared to operate in a contested cyber environment – this can only be verified by testing and evaluation. Developmental T&E includes assessment, verification, and validation of all security controls, including Administrative and Management Controls, Technical Controls, and Operational and Procedural Controls, as well as all performance parameters. Operational T&E determines the effectiveness, suitability, and survivability of the system as a result of the design and security measures implemented. There are a variety of test methods that include, but are not limited to:

- Application of the automated tools/ Security Readiness Review Evaluation Scripts, Security Content Automation Protocol (SCAP), and static code checker/scanner.
- Manual tools to include Defense Information Systems Agency's (DISA) Security Checklists and Security Technical Implementation Guides (STIGs).
- Test tools utilized to test network appliances and related device.
- Software endurance tests.
- Hardware reliability tests.
- Vulnerability scans and penetration tests.
- Operational assessments with live adversary test teams.

Due to the high cost of system testing associated with laboratory use and field assets, it is essential that cybersecurity testing be integrated into routine test objectives and test plans flowing from the TEMP as early in development as possible. Cybersecurity operational and technical requirements should be integrated into standard test objectives and test plans alongside other KPPs, KSAs, and additional performance attributes, so as to leverage system time and execute efficient tests that demonstrate the required performance of the functional design. For programs that are on operational test and evaluation oversight, test plans will be reviewed and approved by the Director, Operational Test and Evaluation (DOT&E) for test adequacy, including cybersecurity testing. DOT&E has provided specific procedures for OT&E of cybersecurity which should be reviewed by the cognizant operational test agency prior to conducting cybersecurity operational testing.[7]

For more info on cybersecurity T&E, see Annex D, Cybersecurity Test and Evaluation Considerations.

2.2.9 Test Plans and Reports

All cybersecurity requirements identified in the RTM need to be traceable through the development process and validated during testing. This includes ensuring that cybersecurity requirements defined in the RTM are traceable to the program's incremental test plans. Early in the test planning process, the ISSM should work with the T&E director to identify certification, developmental test and evaluation (DT&E), and operational test and evaluation (OT&E) events which will satisfy required cybersecurity test objectives in conjunction with scheduled testing.

[7] DOT&E Memorandum: "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs", dated August 1st, 2014

System test plans for routine testing will include cybersecurity test objectives and procedures to ensure an integrated test approach. Detailed test procedures include, but are not limited to:

- Cybersecurity requirements.
- Test methodology and metrics.
- Test procedures.
- Test resources required.

In addition, reporting of cybersecurity tests should include:

- Test results in terms of vulnerabilities identified.
- Demonstrated/estimated operational effects.
- Residual risk if no technical or procedural solution identified.
- Potential risk mitigations (primary and alternate, if available).
- Residual risk once technical or procedural solution is applied.

2.3 Risk and the RMF Governance Structure

As shown in Figure 2, the DoD RMF governance structure implements the three-tiered approach to cybersecurity risk management described in NIST SP 800-39, synchronizes and integrates RMF activities across all phases of the IT lifecycle, and spans logical and organizational entities.

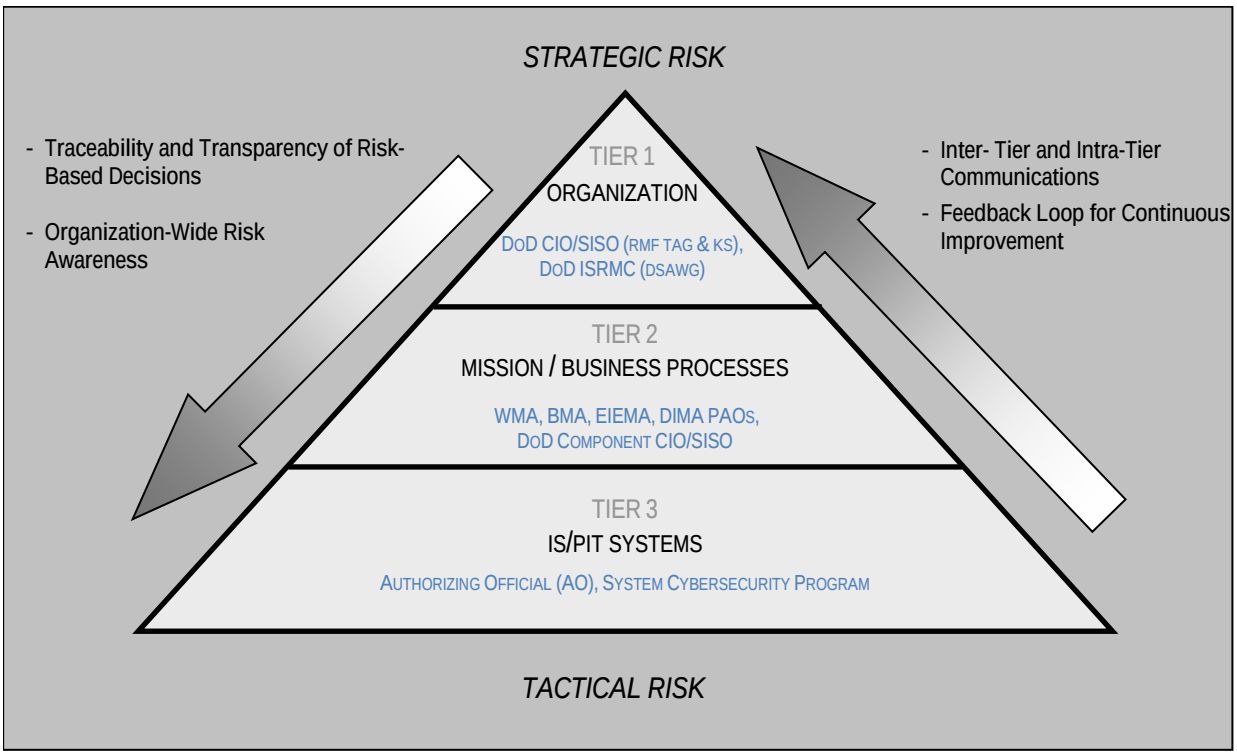


Figure 2. Risk Management Framework Governance

Programs fulfil cybersecurity and system survivability requirements by implementing a tailored set of security controls that are consistent with the risk tolerance of the system determined by RMF authorities. The risk "frame" within the RMF is the set of assumptions, constraints, risk

tolerances, priorities, and trade-offs underpinning the risk management strategy. Risk tolerance is the level of risk an organization is willing to accept in pursuit of strategic goals and objectives, e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable. Risk tolerance drives many of the decisions throughout a system's lifecycle, to include the risk response, i.e., acceptance, avoidance, mitigation, or sharing/transfer. As we move from general to specific through the three RMF tiers, from enterprise to mission/business processes to individual systems, risk tolerance can be expressed in increasing detail.

At the enterprise level, RMF Tier 1, network AOs manage community risk to the Department of Defense Information Networks (DoDIN) and all resident/connecting systems by issuing authorizations to connect. A network AO's risk tolerance is based on ensuring security controls addressing community risk (e.g., intrusion detection, vulnerability management, and patch management) function as intended. Network AOs also address mission risk by incorporating risk tolerance of system AOs, information owners, and mission/business process owners. Both network and system AOs typically have less risk tolerance for more critical information systems than for less critical information systems. Note also that core cybersecurity capabilities should be consistently provided and monitored across all systems over time. As such, it is desirable to align risk tolerance and the enterprise continuous monitoring strategy. In developing that strategy, security automation domains (reference NIST SP 800-137) may be prioritized, with asset management, configuration management, vulnerability management, etc. tending to be higher priorities. While all cybersecurity capabilities supported by the domains are necessary, AOs generally have less risk tolerance for non-compliant security controls supporting higher priority domains.

At the mission/business process level, RMF Tier 2, system AOs and PMs must coordinate with the mission/business process owner/lead and other stakeholders to identify factors consistently present across systems within the mission/business process. Based on the level of concern for the factors, the risk tolerance for each mission/business process can be determined, documented, and communicated to all concerned for consistency in system categorization, in selection and implementation of security controls, and in authorization decisions to operate or interconnect systems within and between mission/business processes.

At the system level, RMF Tier 3, risk tolerance may vary across systems in a mission/business process. As such, AOs must work with program management offices, information system owners, operating organizations, and mission owners to more clearly understand all variables feeding into risk acceptance decisions for specific systems, so that they can express early in the system's lifecycle the system-specific risk tolerance, thereby driving programmatic decisions about which security controls must be selected, implemented, and assessed before an authorization decision will be issued.

For more information on the RMF governance tiers, see DoDI 8510.01, *RMF for DoD IT*, and the RMF Knowledge Service at https://rmfks.osd.mil.

2.4 Resolving Conflict Arising from Cybersecurity Implementation

PMs must take action to resolve conflicts that may arise when implementing cybersecurity and performing RMF processes, regardless of where the system is in the acquisition lifecycle. Resolving issues early in the process can lead to significant cost and time savings throughout the

system lifecycle. Multiple stakeholders may have an interest and multiple coordination efforts may be involved in the process of resolving a conflict.

Figure 3 shows high-level escalation and identifies senior RMF and cybersecurity stakeholders who can assist in resolving cybersecurity conflicts at multiple levels. This chart does not imply a direct chain of command. The acquisition process has a similar communication and governance hierarchy, which is shown on the right hand side of the figure in smaller print.

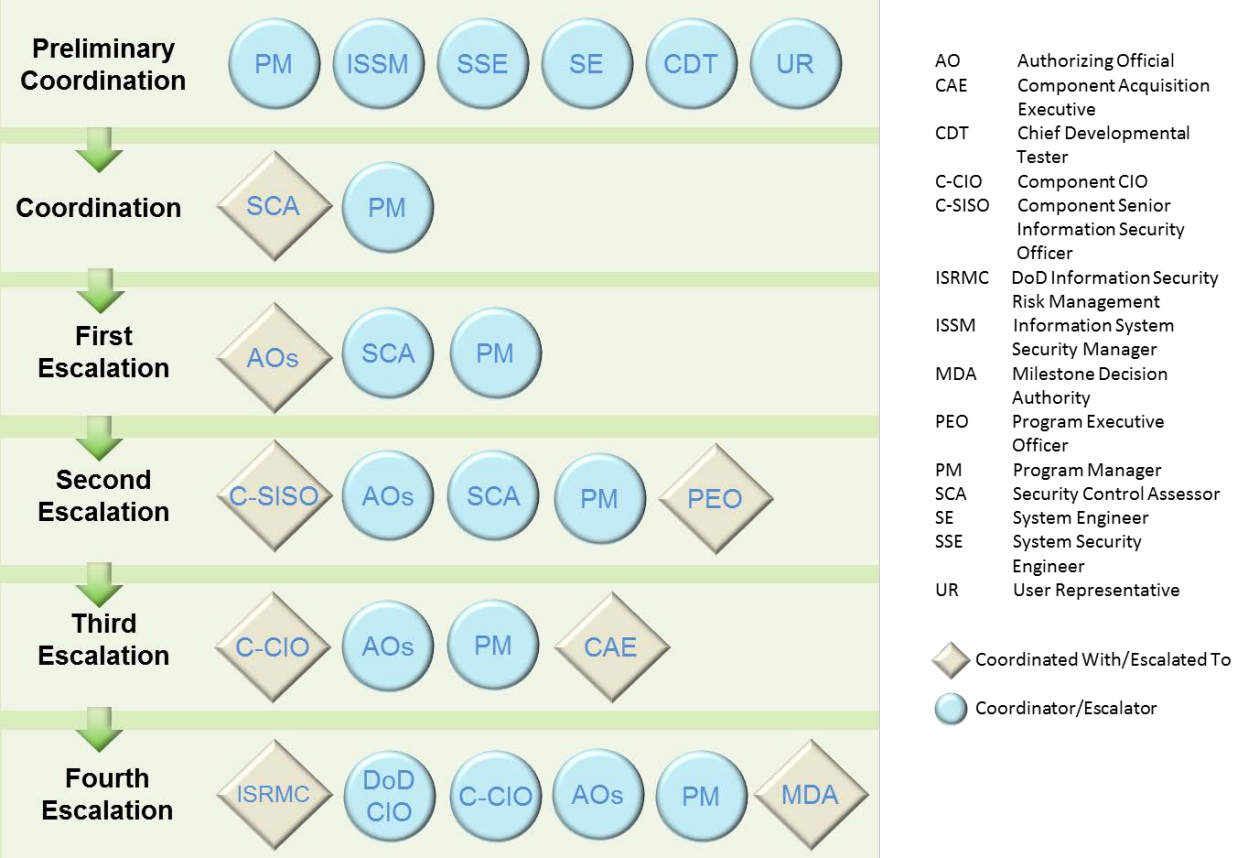
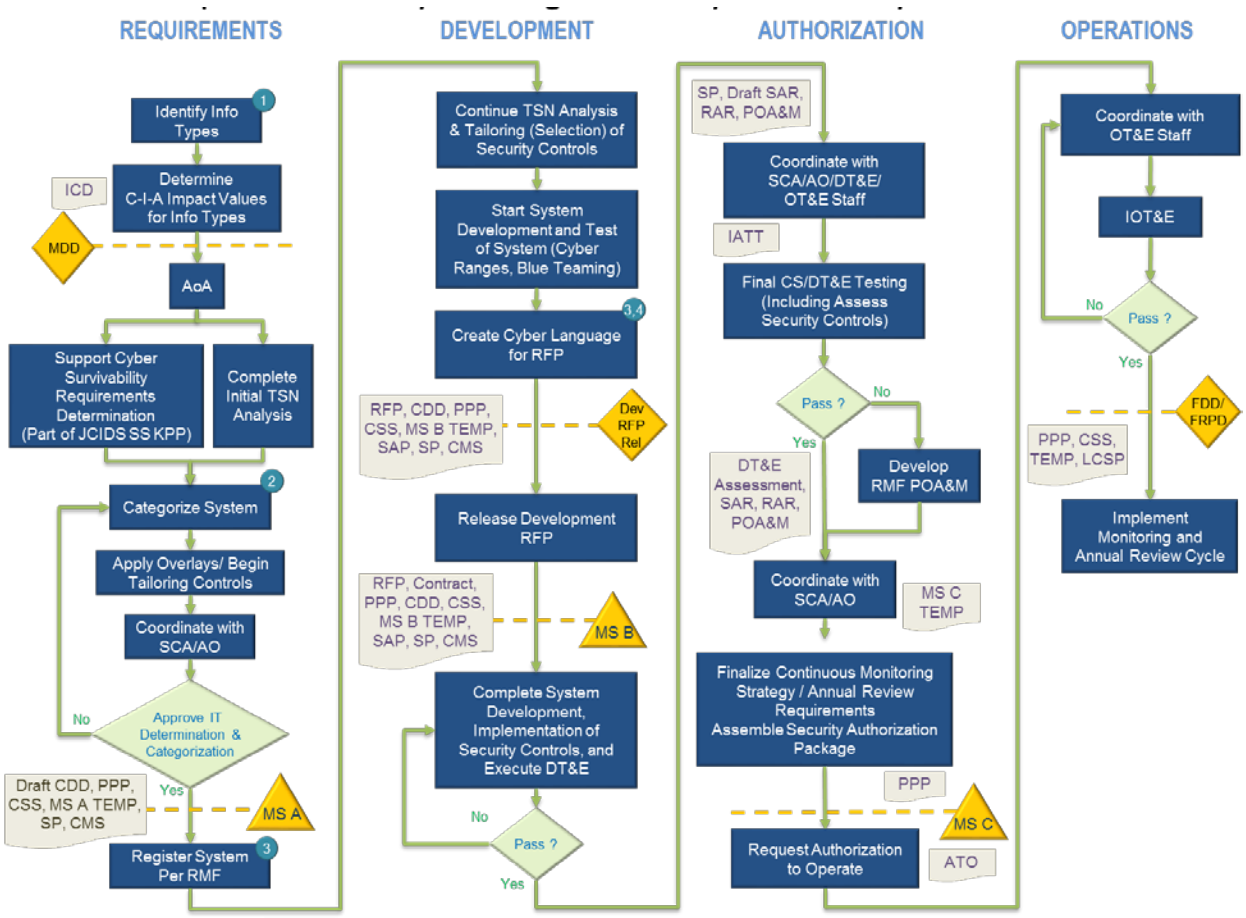


Figure 3. Conflict Resolution

Escalation to the DoD Component CIO may be needed to resolve conflicts between multiple AOs assigned by that CIO or between AOs where one is responsible for managing mission risk (e.g., a "system" authorizing official who issues the Authorization to Operate (ATO)), and the AO responsible for managing community risk (e.g., a "network" AO who issues an Approval to Connect (ATC) to systems with valid ATOs). Escalation is most often contained within a DoD Component; however, when multiple AOs span DoD Components, coordination may be required with DoD-level entities charged with managing community risk (e.g., Defense Information Assurance Security Accreditation Working Group (DSAWG), who issues ATCs), or managing strategic/enterprise risk as the DoD's highest level Risk Executive Function, (i.e., DoD Information Security Risk Management Committee (ISRMC)).

3 Acquisition Lifecycle Cybersecurity Activities and Process Flow

The RMF process provides a method to develop and mature cybersecurity throughout the acquisition lifecycle. Figure 4 illustrates the integration of cybersecurity requirements, the development of the system and its cybersecurity capability, system testing, authorization, and monitoring and maintaining the security state and risk posture. Details are described in sections 3.1 through 3.4.



Key:

AO	Authorizing Official	DT&E	Developmental Test & Evaluation	POA&M	Risk Management Framework Plan of Action and Milestones
AoA	Analysis of Alternatives	IATT	Interim Authorization to Test	SP	Risk Management Framework Security Plan
ATO	Authorization to Operate	IOT&E	Initial Operational Test and Evaluation	SAP	Security Assessment Plan
CCI	Control Correlation Identifier	JCIDS	Joint Capabilities Integration Development System	SCA	Security Control Assessor
CDD	Capability Development Document	KPP	Key Performance Parameter	SS	System Survivability
C-I-A	Confidentiality, Integrity, Availability	OT&E	Operational Test & Evaluation	TEMP	Test and Evaluation Master Plan
CMS	Continuous Monitoring Strategy	PPP	Program Protection Plan	TSN	Trusted Systems and Networks
CS	Cybersecurity	RAR	Risk Assessment Report		
CSS	Cybersecurity Strategy	RFP	Request for Proposal		

References:
1 – NIST SP 800-60 or DoD future document or as a result of Analysis
2 – CNSSI No. 1253
3 – Risk Management Framework Knowledge Service https://rmfks.osd.mil/
4 – See RFP Annex

Figure 4. Acquisition Lifecycle High-Level Cybersecurity Process Flow

3.1 Requirements

The requirements sponsor's (also referred to as mission owner (MO)), and user representative's identification of the preferred alternative from the AoA process triggers many activities in the Materiel Solution Analysis phase leading up to Milestone A (MS A). The system categorization as defined in the RMF is one driver of cybersecurity requirements. Specifically, categorizing the system requires the PMOs, Mission Owners and Information Owners to determine the potential impact to the mission, due to loss or degradation of C-I-A, and capture this impact as distinct values (low, moderate, high) for each information type within the system. Cyber survivability, as articulated in the System Survivability KPP, other KPPs, KSAs, and additional performance parameters are other drivers of cybersecurity requirements. The PM supports the requirements sponsor's and user representative's definition of the cybersecurity requirements in the System Survivability KPP by reviewing the draft Capability Development Document (CDD) for technical feasibility and affordability. The results of the AoA process and the requirements sponsor identification of the preferred alternative trigger an initial TSN analysis. Additionally, the results help determine the initial baseline controls, derived from the final system categorization, and any applicable overlays. Overlays can be considered as an initial "bulk tailoring" activity, but system-specific tailoring of controls is required for all systems.

Initial high-level tailoring starts prior to MS A, but cybersecurity threats and vulnerabilities constantly change; therefore, tailoring must continue throughout the lifecycle. The PM achieves this tailoring by:

- Coordinating the initial security control set with the SCA, and preparing MS A system and cybersecurity documentation.
- Deriving technical requirements for the MS A draft system performance specification based on the draft CDD, CONOPS, architectures and data flows, initial baseline controls after overlays are applied, and other stakeholder requirements.
- Providing cybersecurity input for the draft system performance specification, along with the statement of work, CDRL, and source selection criteria, which are key sections of the Technology Maturation and Risk Reduction (TMRR) RFP at MS A.

For more information, Annex H provides a comprehensive list of cybersecurity considerations in the RFP.

After the AO approves the system's IT determination, e.g., major application, PIT, PIT system, and system categorization as documented in the Security Plan, the PM registers the system and prepares for a MS A decision.

3.2 Development

System definition and initial system design starts after MS A. Systems, technology, and the threat landscape change throughout design and development, which require additional tailoring of controls. Starting from security control baselines, tailoring is based on increasingly robust risk assessments that consider threats, vulnerabilities, likelihood, and potential impact to the mission. Testing, including the use of cyber ranges and blue teaming, starts in the TMRR phase. The TEMP should include cybersecurity testing along with all other testing. During the TMRR phase, when the PM has completed planning for development (i.e., Engineering and

Manufacturing Development (EMD)) and understands the risks, the PM releases the development RFP. RFP release occurs at about the time the System Functional Review is complete and there is an established functional baseline (e.g., system performance specification is final/approved to support preliminary design and implementation of security controls) and the requirements sponsor has validated the CDD. The PM must include cybersecurity language in the development RFP after MDA signs Development RFP release acquisition decision memorandum. The RFP language should identify the correct level of cybersecurity requirements so that the materiel developer will sufficiently protect the information types stored in or used by the system.

The EMD phase includes system development and selection and implementation of security controls. During this phase, more tailoring of controls may be necessary to support detailed design/technical decisions and/or as a response to the changing threat landscape and vulnerabilities requiring risk mitigations. DT&E may be an iterative process; however, the PM must coordinate the final test results with the SCA, AO, DT&E, and OT&E staffs at decision points. The PM should begin drafting the RMF POA&M in response to vulnerabilities documented in the SCA's Security Assessment Report (SAR) and Risk Assessment Report (RAR). The SAR, RAR, and RMF POA&M should leverage the DT&E and any operational assessment results toward the later part of EMD in preparation for Milestone C decision. All of these documents are made available to authorities to determine if the system is ready for final testing.

3.3 Authorization

If it is necessary to test in an operational environment, or to use live data in a test environment, the PM requests an interim authorization to test (IATT) from the AO. To obtain an IATT, PMs and their ISSM must coordinate early and often with the SCA and the AO to determine which artifacts are required and when. The further along a system is in its lifecycle, the more robust the security controls are likely to be and, the more evidence (e.g., DT&E results) the SCA and AO will expect from the PM to prove readiness for testing and to demonstrate the risk of testing is acceptable. Refer to Annex D: Cybersecurity T&E Considerations for more information.

The RMF's security control assessment must be performed by the SCA, but the SCA should leverage results of DT&E to the maximum extent practical. The SCA captures the results of the security controls assessment in the SAR. The SCA also performs a formal risk assessment of non-compliant (or ineffective) security controls and captures the results in the RAR. The PM is usually afforded the opportunity to correct weaknesses before the SCA finalizes the SAR and RAR. The PM provides the approach to mitigate all remaining weaknesses in the RMF POA&M. The AO can ultimately accept or reject proposed approaches, provide conditions, or accept the risk.

At MS C, the PM assembles the system's final security authorization package (Security Plan, SAR, RAR, POA&M), as well as the continuous monitoring strategy and annual review requirements, and submits them to the AO for an authorization decision.

3.4 Operations

If the authorizing official issues an ATO, documented in an Authorization Decision Document (in the Enterprise Mission Assurance Support Service (eMASS)), the PM coordinates with the OT&E staff for operational testing, then OT&E staff conduct IOT&E. Upon successful OT&E, the PM may deploy the system in the operational environment. Deployment initiates system monitoring in accordance with the approved continuous monitoring strategy and/or annual review requirements, as approved by the AO in conjunction with the ATO.

Any change to a system has the potential to negatively impact the cybersecurity posture. In some cases, the change may cause the AO to require re-authorization. The ISSM, in coordination with the SCA, determines the security impact of any changes and if necessary, updates the RMF documentation as required by the SCA and AO. The PM, if assigned lifecycle manager responsibility, is ultimately responsible for maintaining the security posture.

Annex A - Cybersecurity Throughout the Acquisition Lifecycle

Lifecycles of system, product, or service acquisitions containing information technology (IT) can be structured in many different ways, depending on risk and urgency of the need. Some acquisitions will be tailored acquisition programs with acquisition category (ACAT) milestone decision authority (MDA), and others will be acquisitions of services with different decision authorities. MDAs and PMs will tailor and streamline program strategies, oversight, and decision making for acquisition programs to fulfill the specific program needs. In cases of urgent needs, formal milestone events may not be required, and acquisition processes may be modified to expedite delivery.

Figure 5 below, Department of Defense (DoD) Acquisition Lifecycle, is a notional lifecycle based upon DoDI 5000.02, Figure 3, Model 1: Hardware Intensive Program, depicting a high-level view of the time phasing of acquisition and cybersecurity RMF artifacts.

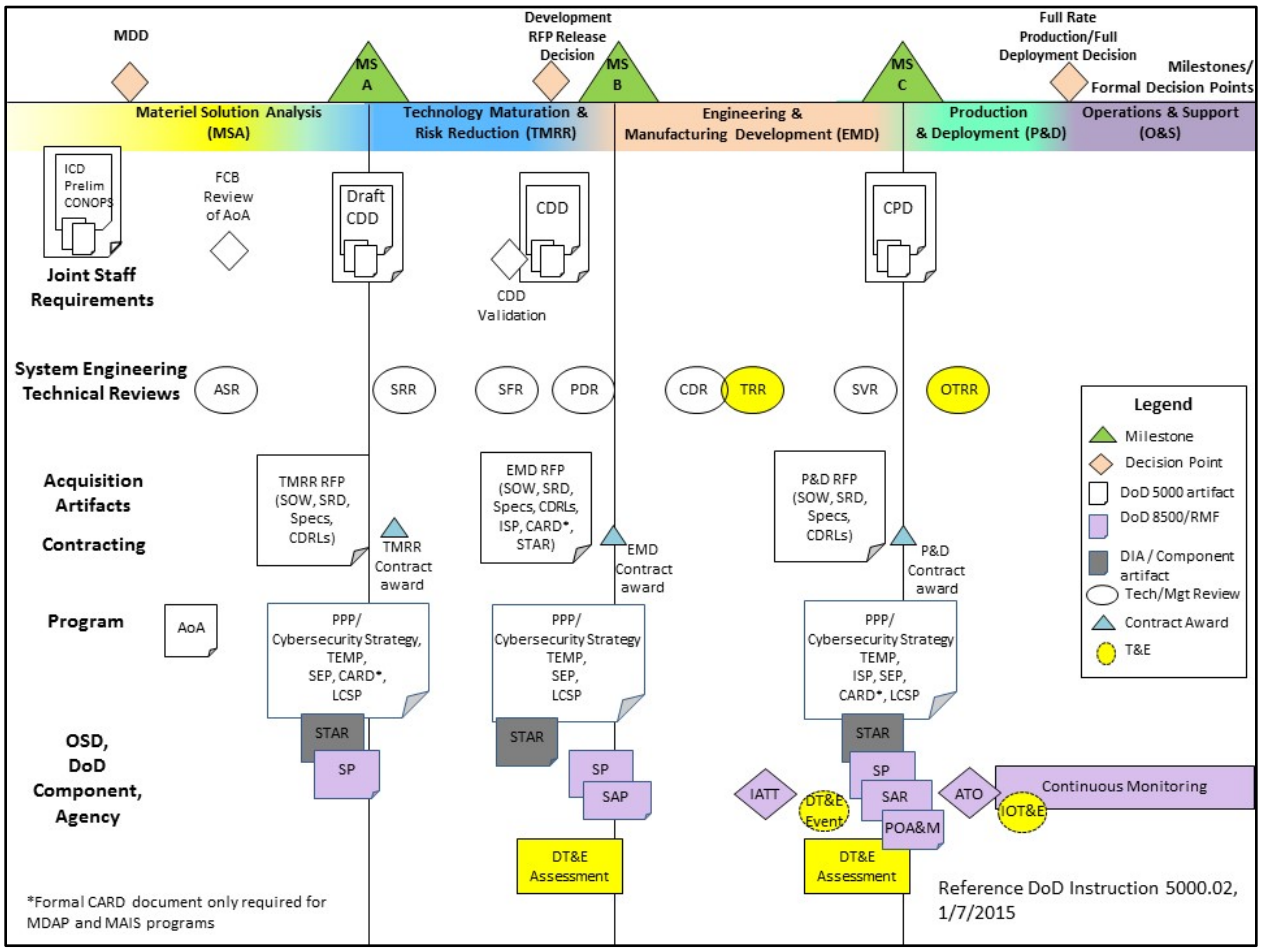


Figure 5. DoD Acquisition Lifecycle

Each program may be structured in a unique way that may or may not include all the activities within the typical acquisition lifecycle or may include additional activities. DoDI 5000.02 provides MDAs the latitude to tailor the lifecycle phases, milestones, and decision review points

and phase content based on specifics of the system, product, or service, as described by the following from the DoDI:

> "The structure of a DoD acquisition program and the procedures used should be tailored as much as possible to the characteristics of the product being acquired, and to the totality of circumstances associated with the program including operational urgency and risk factors.
>
> (a) MDAs will tailor program strategies and oversight, including program information, acquisition phase content, the timing and scope of decision reviews and decision levels, based on the specifics of the product being acquired, including complexity, risk factors, and required timelines to satisfy validated capability requirements.
>
> (b) When there is a strong threat-based or operationally driven need to field a capability solution in the shortest time, MDAs are authorized to implement streamlined procedures designed to accelerate acquisition system responsiveness. Statutory requirements will be complied with, unless waived in accordance with relevant provisions."

A.1 Materiel Solution Analysis (MSA) Phase

The DoDI 5000.02 states that the purpose of the Materiel Solution Analysis (MSA) phase of the DoD acquisition program is to:

- Conduct analysis needed to choose the concept for the acquisition program or system.
- Begin to translate validated capability gaps into system-specific requirements.
- Conduct planning to support a decision on the acquisition strategy for the product.

Figure 6 provides a visual overview of how cybersecurity is integrated into the MSA phase as a foundational part of acquisition, with support from SSE[8] and other functions. Annex G provides additional information on acquisition program artifacts and acquisition-related roles and responsibilities.

A.1.1 Cybersecurity Assessment Criteria for Analysis of Alternatives (AoA)

During the MSA phase, the DoD Component conducts a series of analyses and activities to choose the concept for the capability that will be acquired, and begins to translate validated capability gaps into system-specific requirements and the draft system performance specification. Cybersecurity capability requirements are integrated into the ICD prior to the MSA phase with all other mission capability requirements. Depending on the needs of the system, the cybersecurity capability requirements may be articulated as a KPP, a KSA, or system attributes for the security objectives of confidentiality, availability, and integrity. If cybersecurity capability requirements are not included in the ICD, the level of cybersecurity for the alternative materiel concept studied during the AoA may not be evaluated, and a solution with insufficient cybersecurity may be selected and later designed and built. The Program Management Office (PMO) should establish a Cybersecurity Working-level Integrated Product Team (WIPT) that will develop cybersecurity technical requirements and work with systems engineering throughout the lifecycle;

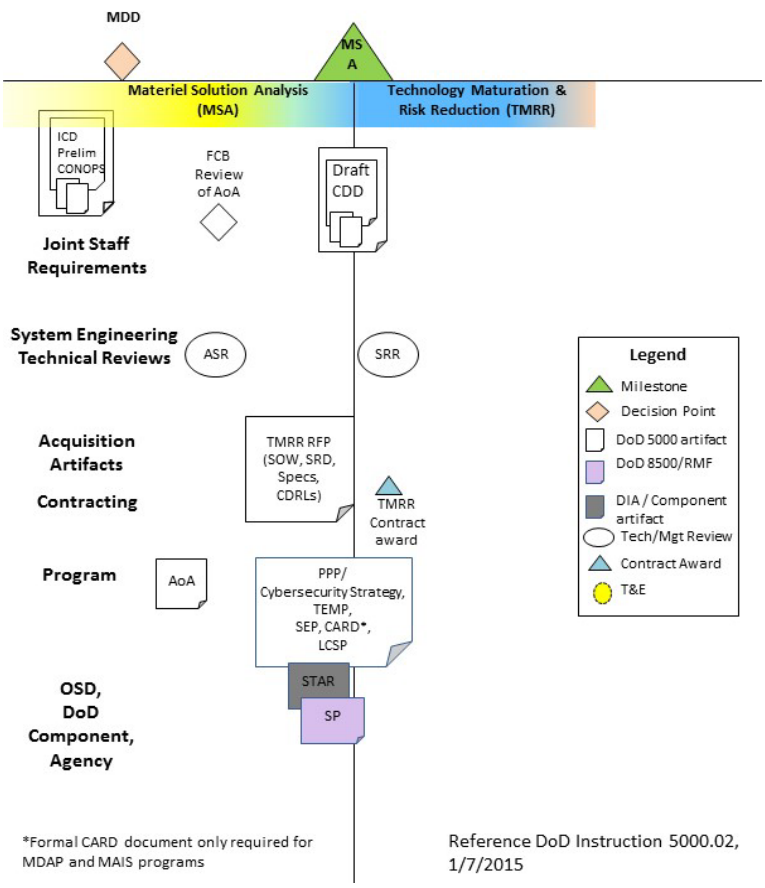


Figure 6. MSA Phase of DoD Acquisition Lifecycle

[8] If necessary, get SSE support from NSA[8] in accordance with DoDI 8500.01. PMs should contact the NSA Client Advocate Chief for more information, at (410) 854-4790

especially early on, before architecture and design decisions are made.

Enterprise architecture features should inform cybersecurity capability requirements in the ICD (e.g., cyber resiliency). Adding cybersecurity into the solution architecture/design up-front is more cost-effective than building it in later in the lifecycle after risk-based cost/design/performance trades have been made. During the MSA phase, the cybersecurity risk assessment focuses on potential mission impact due to the loss of confidentiality, integrity, and availability, not the likelihood of a threat exploiting a system's vulnerability. Ideally, the confidentiality, integrity, and availability impact values (high, moderate, or low) are documented in the ICD or equivalent document, are integrated into and considered throughout the execution of the various analyses, and support the development and selection of a preferred alternative.

Top-level cybersecurity capability requirements are expressed in the system categorization. Under the previous DIACAP information assurance process, the system categorization was articulated as the MAC and CL. Under the RMF, the system categorization is portrayed as impact levels for the security objectives of integrity, availability, and confidentiality. In some cases in the past, this determination was subjectively made, not an objective decision based on an assessment of potential loss of integrity, availability, and confidentiality on the system's mission as intended. Incorrectly establishing the system categorization often impairs the performance of the system and ultimately increases the cost and resources needed to achieve its mission. Reasons for this subjectivity were often due to 1) higher MAC and CL level programs having a better success rate at securing funding in completion with other programs, and 2) justifying a lower level that could be afforded based on the limited funding being allotted to the program. The first case results in over-protecting the information and system. The second case results in under-protecting the information and system. Neither case is desirable. The RMF provides an objective approach to determining this level based on risk and impact on the mission due to loss of integrity, availability, and confidentiality. NIST SP 800-60 - *Guide for Mapping Types of Information and Information Systems to Security Categories*, can help the acquisition and cybersecurity communities more objectively determine the level of required cybersecurity: integrity, availability, and confidentiality. This initial cybersecurity level drives the initial baseline of required security controls, as the starting point for tailoring throughout the system lifecycle.

These cybersecurity risks are identified through cybersecurity risk assessments that occur throughout the acquisition program lifecycle. The most appropriate risk assessment approach during this phase is a qualitative model, as many of the system details necessary for a more quantitative approach have not been defined or are not yet available. For example, the solution's technology is usually not yet selected at this point; therefore, the technical vulnerabilities cannot be known. For similar reasons, the most appropriate analysis approach is the threat-oriented approach or the asset/impact-oriented approach. Some of the studies and analyses that may have potential cybersecurity implications are the affordability analysis, cost analysis, early systems engineering analyses, threat projections, sustainment considerations, and market research. The cybersecurity risk of materiel solution alternatives will be assessed during the AoA and considered when selecting the preferred alternative.

SSE activities, including cybersecurity, need to be integrated into the program throughout the acquisition lifecycle. Countermeasures associated with the other SSE specialties (e.g., software

assurance) mitigate cybersecurity as well as other system security risks to the program or system, including the system's development environment as well as the operational system's critical functionality and components and Critical Program Information (CPI). Because program resources are limited, systems engineering trade-offs need to be made, and mitigations implemented commensurate with the identified levels of system security risks. The program manager should ensure that the AO is involved in the review of the acquisition documentation that includes cybersecurity requirements related to security controls (e.g., statements of work and system requirements documents in RFPs and specifications), and that the AO (or their designated representative) participates in systems engineering trade-offs, milestone reviews, and decision reviews.

The PM works with the requirements sponsor[9] and user representative to understand the cybersecurity aspects of the operational mission, capability gaps, and the preliminary Concept of Operations (CONOPS) based on the validated ICD. This operational information will help the PM understand the true capability requirements and better develop a solution with the level of cybersecurity necessary to meet those requirements. The system specifications and ultimate success and validation of the program are based on tracing up to and meeting these user cybersecurity capability needs. (See Figure 7)

If required by the AoA Study Guidance and Plan, the impact values for C-I-A, and any other cybersecurity capability requirements in the validated ICD serve as the basis for the assessment of cybersecurity in the AoA. During the AoA, the PMO may be asked to support the assessment of cybersecurity risks based on the physical and operational environment of each potential materiel solution alternative and specific-system characteristics.

A.1.2 Develop Initial Cybersecurity Strategy and Include Cybersecurity in MS A Documentation

After the AoA is complete, the impact values for confidentiality, integrity, and availability are analyzed for any changes based on the preferred alternative and documented in the draft CDD to baseline the initial cybersecurity requirements and form the initial security controls baseline.[10] If a security control overlay exists for a capability the program intends to implement, the overlay should be applied after the AoA is complete.[11] Overlays are bulk tailoring developed and agreed to in advance based on an assessment of risk for a particular type of information, system function, or operating environment. Overlays provide the justification for security control specifications that can be leveraged to expedite or ease the burden of system-specific tailoring. Overlays are applied to the security control baseline resulting from security categorization to form the initial security control set, which should be documented in an initial Security Plan.[12]

---

[9] Sometimes referred to as Mission Owner or Program Sponsor

[10] The system technical initial security controls baseline traces to the preliminary system performance specification, which is part of the preliminary functional baseline.

[11] For example, if utilizing a Cross Domain Solution (CDS), the program should utilize the CDS Overlay when selecting the security controls for the system. DoDI 8500.01 and CJCSI 6211.02 may require additional activities for Information Systems implementing a CDS.

[12] The Information System Security Manager (ISSM), with assistance from the PM, information owner, requirements sponsor, user representative, and SSE, develops the initial Security Plan that is approved by the authorizing official.

This initial security control set is the starting point for system-specific tailoring.[13] System-specific tailoring of the initial security control set requires a risk assessment to determine if threats may exploit vulnerabilities; therefore, it informs which controls must remain in or be added to the initial security controls baseline to mitigate the identified risks.[14] Special security considerations, including cross domain solutions (CDS) and communications security (COMSEC)-related requirements, should also be addressed through the tailoring process.

An initial cybersecurity risk assessment reveals which controls are deemed "not applicable" and are documented in the Security Plan with a supporting rationale to show that no relevant threats are projected to be able to exploit known or projected vulnerabilities. As technology choices are solidified and more is known about the related vulnerabilities, the risk analysis can move from a threat-oriented approach to a vulnerability-oriented approach. The Security Plan is an RMF artifact providing an overview of the cybersecurity capability requirements and the technical requirements for the system, and describes the planned security controls to meet those requirements.

Aligning the system solution conceptual architecture/design with applicable enterprise cybersecurity architectures will allow any common enterprise cybersecurity capabilities to be inherited, eliminating the need to develop and implement a system-unique cybersecurity capability and reducing DoD enterprise cybersecurity risk and system cost. The PM performs requirements analysis and cybersecurity risk assessments, with input from the Sponsor and AO, to develop mitigations to determine the most cost-effective and affordable preferred alternative that satisfies the functional capability requirements. Once the preferred alternative is selected, it becomes the basis for the cybersecurity requirements and specifications for the system that will be developed, built, and deployed.

The Cybersecurity Strategy[15] is developed and iteratively updated and refined to reflect both the program's long-term approach for, as well as its implementation of, cybersecurity throughout the program lifecycle. It also describes the program's approach for completing cybersecurity risk assessments (including current and projected threats and vulnerabilities), which should support requirements analyses, trade-offs, and mitigations throughout the lifecycle of the program. The Cybersecurity Strategy is approved and appended to the Program Protection Plan (PPP). The acquisition and cybersecurity communities coordinate early and throughout the lifecycle on the level of cybersecurity included in the system architecture/design, and ensure this information is reflected in the Cybersecurity Strategy. This coordination will ensure that the official assessing cybersecurity risk of the design prior to testing and deployment understands and can communicate the risks to the system introduced by design trades that affect cybersecurity. This coordination will help to ensure cybersecurity risks are acceptably addressed and will allow for a timely authorization to operate (ATO).

---

[13] The more the system's characteristics and the assumptions about its operating environment deviate from the assumptions stated in Committee on National Security Systems Instruction (CNSSI) No. 1253, the more likely it is that the security controls need to be tailored. This is because the CNSSI No. 1253 baselines were built against the stated assumptions (i.e., assumed a typical information system).

[14] If a specific risk model exists for the capability the program intends to implement, that risk model should be used when performing the risk assessment.

[15] The Cybersecurity Strategy was previously called the Acquisition IA Strategy.

A system-level Continuous Monitoring strategy is initially developed while defining cybersecurity requirements and selecting and tailoring the corresponding security controls during MS A. The strategy defines how security controls will be monitored over time for effectiveness. If controls were selected that cannot be monitored, the PMO is advised to select equally effective, but different or compensating controls that can be monitored. To ensure integration and alignment with enterprise efforts, the system-level strategy aligns with the DoD Component and DoD-level continuous monitoring strategies. The system-level strategy ensures the capability is built-in during the lifecycle phases for cost-effective cybersecurity situational awareness, and to protect the information and system, detect threats, react to incidents, and restore system capability. The strategy discusses how to monitor security controls employed within or inherited by the system, and how to monitor proposed or actual changes to the system and its environment of operation. The strategy includes the plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor. The breadth, depth, and rigor of these annual assessments reflect the system categorization and threats to the system.

The AO[16] (or designee) reviews and approves the Security Plan and system-level continuous monitoring strategy. By approving the Security Plan, the AO agrees to the system categorization, the set of security controls proposed to meet the cybersecurity requirements for the system (and thereby mitigate risk), and the adequacy of the system-level continuous monitoring strategy. The approval of the Security Plan also establishes the level of effort required to complete the remaining steps in the RMF and provides the basis of the system cybersecurity for the acquisition of the system, subsystems, and components.

To understand the cyber threats applicable to the program and ensure the planned security controls and protection mitigations address these threats, the PMO works with the DIA or the Component Intelligence entity to solicit future threat sources to support development of systems that are secure against likely threats that the system will face during acquisition and when deployed and operational. Adversary threat capabilities against the system are captured in the System Threat Assessment Report (STAR) or equivalent document. Use of current threat sources supports ongoing cybersecurity risk assessments and vulnerability assessments to ensure the system retains the required level of cybersecurity.

PEOs/PMs should engage their supporting intelligence representative and/or agency early in the acquisition lifecycle to determine their intelligence requirements IAW DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection within the Research, Development, Test, and Evaluation (RDT&E)*; and DoDI 8500.01, *Cybersecurity*.

To address the affordability of the planned cybersecurity protections, the PM ensures cybersecurity cost estimates are included in the CARD or equivalent information supporting cost estimation for the program.

SSE and program protection and cybersecurity planning inform the PPP, Cybersecurity Strategy, and other MS A program planning and cost documentation, the draft CDD, and the draft TMRR

[16] See the list of roles and responsibilities in Annex A for information about the AO.

RFP. All of the MS A documentation and the Security Plan incorporate risk-based, mission-driven cybersecurity considerations and remain aligned throughout the acquisition lifecycle. As cybersecurity technical requirements are derived, decomposed, and allocated to the system architecture and design at various levels of abstraction, it is essential to document and maintain traceability of the technical requirements to the security controls (see Figure 7).

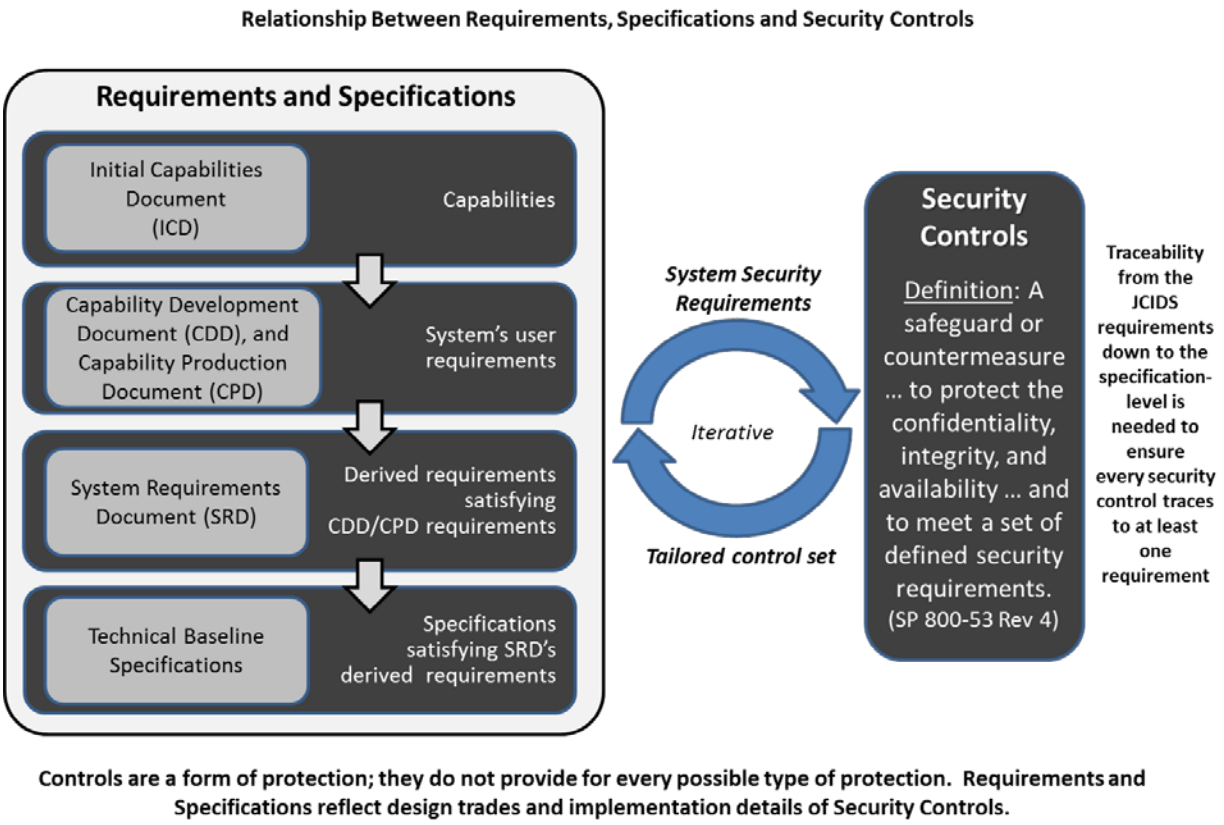


Figure 7. Relating Capabilities/Requirements/Specifications and Security Controls

Annex B provides a matrix illustrating roles and responsibilities (responsible, accountable, supportive, consulted, and informed) of the various stakeholders throughout the acquisition lifecycle. Annex G lists the required products per milestone or decision point with associated approval authorities and responsibilities. Products can be tailored as applicable to meet the unique needs of a program.

The RMF artifacts (e.g., Security Plan, Security Assessment Plan, Security Assessment Report [SAR], Plan of Action and Milestones [POA&M]) should be developed by or in concert with the acquisition community and PMs may choose to stand up IPTs to support such efforts. This planning helps the PM transition to the TMRR phase and begin system requirements analysis and initial system design with good initial cybersecurity capability requirements and initial security controls baseline to flow down and further tailor based on cybersecurity risk assessments. The PM should open the lines of communication with the Component CIO community, the AO, the requirements sponsor, and the user/operational community early in the lifecycle to promote

coordination and cooperation among offices, ensuring the stakeholders effectively design cybersecurity into the system.

A.2 Technology Maturation and Risk Reduction (TMRR) Phase

In the Technology Maturation and Risk Reduction (TMRR) phase, depicted in Figure 8, activities include competitive sourcing, technology development demonstrations, and additional design and requirements trades. The PM achieves cybersecurity risk reduction through a series of activities that help ensure an affordable product, and executable development, production, and sustainment programs.

A.2.1 Include Cybersecurity in System Design and Development RFP Release Decision Documentation

At the beginning of the TMRR phase, the PMO applies a systems engineering approach to elicit, analyze, and decompose capability requirements into technical solution requirements and specifications. This provides the basis of the technical design and includes cybersecurity requirements. The PM coordinates with the requirements community to understand the cybersecurity requirements and provides feedback on the draft CDD. CDD validation is performed later in the TMRR phase.

As the systems engineering process is applied, the set of security controls continues to be tailored[17] to address system-specific cybersecurity risk and performance considerations.[18] Tailoring supports the development of the system performance specification, item performance specifications, and preliminary design. The tailored set of security controls is documented in the Security Plan.

After the Security Plan is developed and refined, the PM determines whether the program is ready to start system-level

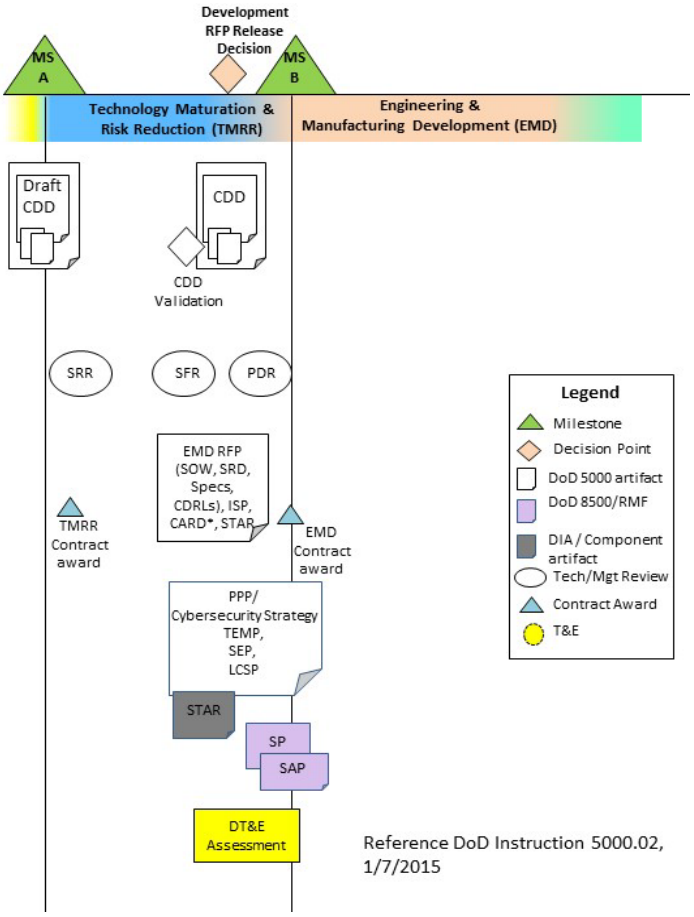


Figure 8. TMRR Phase of DoD Acquisition Lifecycle

[17] Annex C provides more detail about the SSE process and controls tailoring.

[18] The more details that become known about the system's IT, the more the analytic approach can move from a threat-oriented approach to a vulnerability-oriented approach. The risk assessment approach can also become more quantitative than qualitative.

design through a System Requirements Review (SRR). This review produces a solid understanding of the top-level system requirements that supports further requirements analyses, technical design, and technology and cybersecurity risk reduction activities.

Requirements definition provides input to the program's plans for T&E. T&E planning takes into account cybersecurity requirements and security control assessments and is performed in collaboration with the SCA, who is responsible for the development of the Security Assessment Plan. The advantages of this collaboration include achieving a broader, more holistic view of the program's T&E effort, thereby promoting reciprocity for testing activities, and gaining a better understanding of the schedule and resource requirements.

Cybersecurity requirements are included in system performance requirements, and as such they should be clearly articulated in the functional baseline. The System Functional Review (SFR) determines if the system's functional baseline fully captures the necessary performance requirements and functions, and whether the program is ready to begin preliminary design with an acceptable degree of risk. When reviewing the system performance and functionality, the PMO ensures appropriate cybersecurity requirements are included and the system's ability to withstand cyber threats is integrated and balanced with other performance requirements comprising an efficient and effective operational system.

The requirements sponsor will validate the CDD (or equivalent requirements document) for the program. This validation will precede the Development RFP Release Decision Point and provide a basis for preliminary design activities and the Preliminary Design Review (PDR) occurring prior to MS B.

In preparation for the Development RFP Release Decision Point, documentation is updated in coordination with and informed by available cybersecurity artifacts, including the Cybersecurity Strategy, Security Plan, and Security Assessment Plan.

At the Development RFP Release Decision Point, the PM summarizes TMRR phase progress and results, and reviews the Acquisition Strategy for the Engineering and Manufacturing Development (EMD) phase. The Acquisition Strategy includes specific cybersecurity considerations that may impact the overall affordability of the system, the competition strategy and incentive structure, engineering and supportability trades and their relationship to validated capability requirements, the threat projections applicable to the system, risk management plans, and the basis for the program schedule. These specific cybersecurity considerations are put in the RFP language and built into the program.

A.2.2 Include Cybersecurity in Preliminary Design and Final MS B Documentation

A PDR is completed before MS B and prior to the contract award for EMD to reduce program risks, including risks related to cybersecurity. An important part of the preparation for the PDR is the definition of the allocated baseline. The allocated baseline describes the functional and interface characteristics for all system elements, including cybersecurity, and the verification required to achieve these specified characteristics. The functional and interface characteristics are allocated and derived from the higher level architectures in the Information Support Plan (ISP) as well as the ICD, draft CDD, and other products. From a cybersecurity perspective, this

activity ensures cybersecurity technical requirements are adequately addressed. T&E will prepare and provide a preliminary DT&E assessment in support of the PDR just prior to MS B.[19]

Upon completion of the Development RFP Release Decision and PDR, the PMO will turn its attention to making final preparations for the MS B review and decision. It also commits the required investment resources to the program. Most requirements for this milestone should be satisfied at the Development RFP Release Decision Point; however, if any significant changes have occurred, or if information not available at the Development RFP Release Decision Point could impact this decision, it is provided at MS B. MS B requires final demonstration that risks, including cybersecurity risks, have been adequately mitigated to support a commitment to design for production. The RFP and the subsequent contract should define the process the government will use to review and assess system performance (that includes cybersecurity). Cybersecurity is part of the validated capability requirements; it must have full funding in the Future Years Defense Program and comply with affordability goals for production and sustainment considered at MS B.

[19] For more information on the regulatory and statutory requirements for conducting and reporting on a PDR, see Table 5 in Enclosure 1 of the DoDI 5000.02.

A.3 Engineering and Manufacturing Development (EMD) Phase

The purpose of the Engineering and Manufacturing Development (EMD) phase is to develop, build, and test a product to verify that all operational and derived requirements have been met and to support production and deployment decisions. The EMD phase is illustrated in Figure 9. The PMO will complete the detailed designs for the product's hardware and software, systematically close any open risks, build and test prototypes to verify compliance with requirements, and prepare for production and deployment.

A.3.1 Include Cybersecurity in Detailed Final Design

Cybersecurity requirements are mapped and allocated to the hardware and software design for the system as part of the overall system development process. This mapping is based on risk assessments identifying which threats may exploit vulnerabilities in the chosen hardware and software.[20] These technology choices may bring unanticipated risk, and additional security controls may need to be allocated to components to adequately mitigate identified risk. The PMO continues to coordinate with the requirements/functional sponsors as engineering and program trades occur that might affect the resulting cybersecurity capabilities in the delivered system.[21]

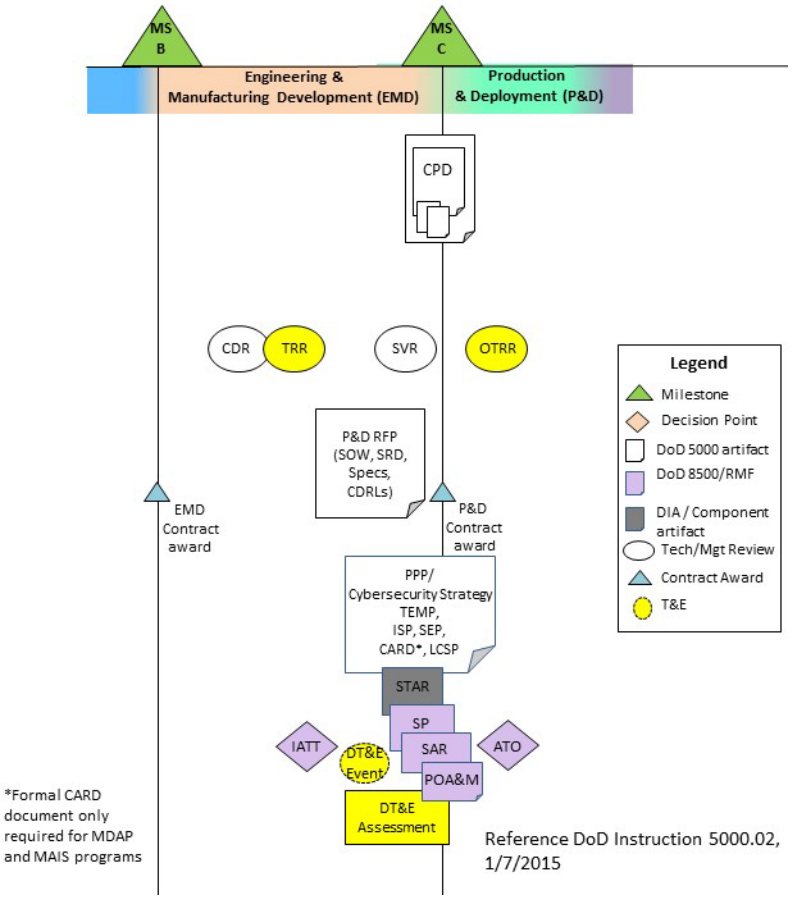


Figure 9. EMD Phase of DoD Acquisition Lifecycle

To start the process, the PMO establishes coordination and collaboration between SSE and developers. The objective is to ensure developers understand relevant threats and development will be conducted in accordance with security controls related to assurance, system development, and cybersecurity best practices to reduce vulnerabilities and to design, build, and test cybersecurity in the system early and cost effectively. Systems engineering completes the detailed build-to design of the system, ensuring cybersecurity

[20] As more details about the system's IT are known at this point, the risk assessment can move from qualitative to semi-quantitative or quantitative. Also, the analytic approach can move from a threat-oriented approach to a vulnerability-oriented approach.

[21] In addition, the PMO coordinates with the appropriate authorizing officials to perform all assessment and authorization activities necessary to obtain appropriate approvals and authorizations (such as an Interim Authority To Test [IATT]) to conduct system testing activities.

requirements are met. This systems engineering includes technical planning as defined in the approved Systems Engineering Plan (SEP) and verifies compliance with the functional, allocated, and product baselines. The T&E and cybersecurity assessment communities align the Security Assessment Plan with the T&E Master Plan to ensure integration of cybersecurity assessments into DT&E. DT&E of system elements and the system (where feasible) demonstrates system maturity and readiness to begin production and OT&E and/or deployment and sustainment activities.

As part of the overall system development, the PM ensures cybersecurity requirements are mapped and allocated to the hardware and software design. All software code development should be assessed for secure coding practices and standards,[22] with an emphasis on compliance with software development standards throughout the development process. The PMO tracks and updates cybersecurity risk mitigation activities and refines the PPP. These mitigation activities are based on Trusted Systems and Networks (TSN) analysis[23] and cybersecurity risk assessments and inform the coordinated tailoring of controls and design trades. The results of these analyses are documented in the Security Plan. Cybersecurity risk assessments can leverage TSN analyses, which are included in program protection activities conducted throughout the acquisition lifecycle, at systems engineering technical reviews and milestone reviews and decision points. The PM also coordinates with stakeholders on T&E activities, the mitigation of exploitable vulnerabilities discovered during DT&E, and evolving requirements.

T&E continues, based on the evolving requirements and preliminary and detailed design. The T&E community, in collaboration with SSE, characterizes the attack surface[24] to assess cybersecurity in component and system integration testing. This could be early contractor testing, government DT&E, or a combination based on the program TEMP.[25]

The PMO refines the PPP to reflect any changes to risks and countermeasures to mitigate them and documents cybersecurity risks known to date, based on the most current threat and vulnerability assessments. As part of the TSN analysis, the Threat Assessment includes obtaining threat assessments from the DIA Supply Chain Risk Management (SCRM) Threat Analysis Center (TAC) via the TSN focal point for suppliers of critical components. If new or updated threat assessments reveal threats not accounted for in previous risk assessments, the risk assessment is updated. If unacceptable risks are identified, security controls, countermeasures, and/or requirements baselines may need to be updated to mitigate the risk to an acceptable level, based on feedback from authorizing officials. The PMO reviews the program's cybersecurity engineering requirements to ensure they are executable within the existing budget.[26]

All required cybersecurity features of the program are reflected in an updated CARD (or equivalent document) based on the system technical baseline. The program schedulers update

---

[22] For more information, see Defense Acquisition Guidebook (DAG), Chapter 13.
[23] For more information, see Annex C.
[24] Because the system architecture products alone do not provide all necessary information on interfaces and data exchanges, additional products such as network diagrams may be needed to characterize the attack surface.
[25] For more information on T&E activities and the TEMP, see DAG, Chapter 9.
[26] For more information on how to leverage and map the SSE-related activities into the Milestone C PPP and other related documents, see DAG, Chapter 13, Program Protection.

the program schedule to reflect cybersecurity activities, including critical path drivers. Program analysts review the adequacy of cybersecurity processes and metrics to ensure they are in place for the program to succeed in operation. The PMO reviews program staffing for cybersecurity going forward to deployment and sustainment.

During this phase, a Critical Design Review (CDR) is conducted to assess the design maturity, including cybersecurity, build-to or code-to documentation, and remaining risks, leading to the establishment of the initial product baseline. The CDR is the decision point to assess and confirm the adequacy of the system design to meet the system requirements, including cybersecurity, and readiness to begin developmental prototype hardware fabrication and/or software coding with acceptable risk. The PMO ensures CDR entrance criteria for cybersecurity baseline design are met and all cybersecurity requirements are reflected in the product baseline, which includes the design. In support of the CDR, DASD(DT&E) provides an assessment of DT&E performed to date, including cybersecurity, for programs on the OSD DT&E oversight list.

Decomposed component specifications, with inherent cybersecurity requirements, are fully defined, including verification criteria, and traced to the security controls documented in the Security Plan. The PM may be responsible for managing software development activities that incorporate code reviews and architecture reviews against incremental builds to reduce vulnerabilities in any custom software, including via automated scanning tools (e.g., static analysis). Code and architecture reviews are informed by the TSN criticality, vulnerability, threat, and risk analyses. The system's security controls are assessed against the Security Assessment Plan using appropriate procedures to determine the extent to which the controls are effective, operating as intended, and producing the desired outcome with respect to meeting the cybersecurity requirements for the system. The assessment of the security controls is documented in a SAR and provided to the testing community and the PMO to determine the appropriate follow-up action (e.g., proposed risk response in the POA&M).

During the EMD phase, the PM should ensure that DoD-evaluated and certified/approved products are employed. This step includes using hardware from the Defense Information Systems Agency (DISA) Unified Capabilities (UC) Approved Products List (APL), and software that has undergone National Information Assurance Partnership (NIAP) evaluation and has been published on the Approved Products Compliance List (APCL). The Common Criteria Evaluation and Validation Scheme (CCEVS) and the Unified Capabilities Requirements (UCR) are intended to complement each other in scope and capability with minimal overlap.

The DISA-published DoD UC APL is a single consolidated list of products that have completed interoperability and cybersecurity certification. Use of the DoD UC APL enables DoD services and agencies to purchase and operate UC systems (primarily hardware) for connection to DoD networks. Security assessment and authorization are streamlined for UC-approved products. The APL is documented in the Approved Products List Integrated Tracking System, which is updated regularly and available at https://aplits.disa.mil/processAPList.do. The UC APL primarily includes network and communication-related services.

The CCEVS products address a broad spectrum of IT products, including operating systems, database management systems, common applications, security products, and several

communication products. Because NIAP-compliant products are evaluated and published on a NIAP-CCEVS APCL, security assessment and authorization is streamlined when compared to using non-evaluated products. The vendors are required to ensure that their products are updated and evaluated upon the release of updated versions and security patches. The NIAP CCEVS program is a partnership between the U.S. government and industry.

A.3.2 Test Cybersecurity Requirements in a Cyber Threat Environment and Assess Cyber Risk to Support Initial Deployment Decision

Following the CDR, the PM also coordinates with the authorizing official to obtain an authorization decision (i.e., IATT) to assess the system within an operationally realistic environment, prior to MS C, for inclusion in the DT&E assessment. To obtain an IATT (for testing in an operational environment, or when using live data in a test environment), PMs (leveraging their ISSM) must coordinate early and often with the SCA's and the AO's offices to determine which artifacts are required and when. The intent is for all applicable security controls to be tested and satisfied before testing in an operational environment or with live data except for those that can only be tested in an operational environment. While most IATTs are issued shortly before MS C, when development is nearly finalized, it is possible an IATT for the system or its components is necessary earlier in the lifecycle. In this situation, not all security controls may have been fully implemented or tested, thereby generating evidence of effectiveness; therefore the risk of testing in an operational environment or with live data may not be fully known. Regardless, all cybersecurity documentation (proving security control effectiveness and conveying risk) that can be generated must be generated as early as possible and made available to support the IATT decision. The farther along a system is in its lifecycle, the more robust the security controls are likely to be and the more evidence (e.g., DT&E results) the SCA and AO will expect from the PM to prove readiness for testing and to demonstrate the risk of testing is acceptable. A Test Readiness Review is conducted to evaluate whether the product or system under development is ready for further DT&E. During this phase of DT&E, the system should undergo a vulnerability assessment, and the system's implementation of cybersecurity requirements should be evaluated in a mission context using realistic threat exploitation techniques. This effort supports the formal validation of the CPD. Note: those systems under DOT&E oversight will be required to conduct an Operational Assessment, which supports the first limited fielding for acquisition. The PM implements and verifies cybersecurity-derived requirements in the hardware and software design for transition to the development and manufacturing environment. Prior to MS C, the PMO completes cybersecurity DT&E and a Functional Configuration Audit/System Verification Review/Production Readiness Review.

A.4 Production and Deployment Phase and Operations and Support Phase

The Production and Deployment (P&D) and Operations and Support (O&S) phases mature the initial product baseline through production/ deployment, operations, sustainment, and disposal. The P&D and O&S phases consist of the following program activities:

- Initial production or limited deployment/ fielding
- OT&E
- Lifecycle sustainment
- Disposal

Figure 10 illustrates which key artifacts are required for integrating cybersecurity into the P&D and O&S phases. Integration of the cybersecurity RMF early and throughout the acquisition lifecycle is essential to obtaining an authorization to operate (ATO) decision in the P&D phase prior to initial operational test and evaluation (IOT&E). The initial security controls baseline is developed during the MSA phase, and the set of security controls is tailored throughout the acquisition lifecycle. Verifying that security controls are properly implemented prior to OT&E will reduce cybersecurity vulnerabilities and avoid common problems.[27]

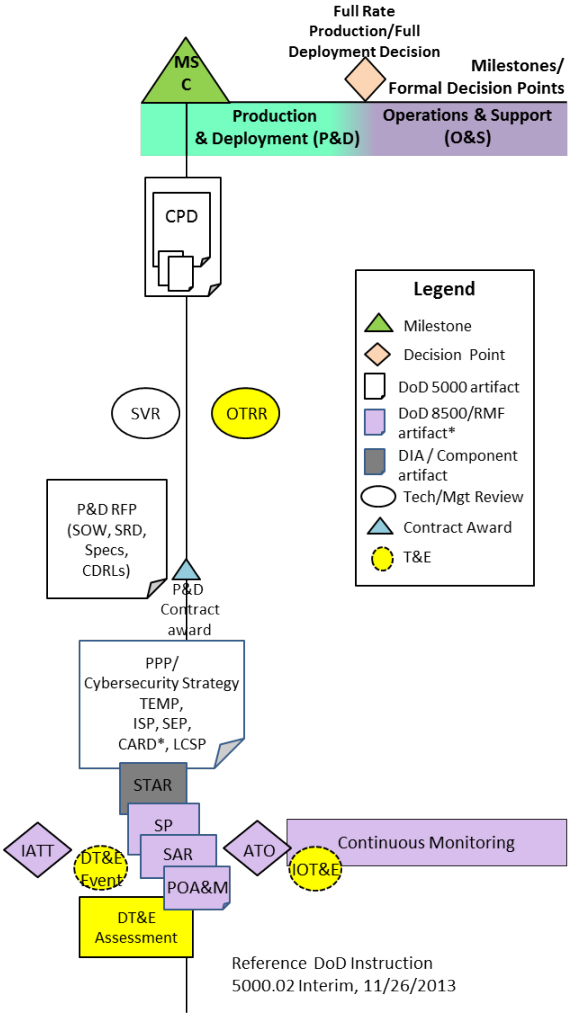


Figure 10. P&D O&S Phases of DoD Acquisition Lifecycle

A.4.1 Production and Deployment: Operationally Test Cybersecurity to Support Full or Final Deployment Decision

An ATO may be required prior to IOT&E, if the testing is conducted in the operational environment or on deployed capabilities. In addition, the program must obtain interoperability certification[28] and approval to connect[29] to the DoDIN.

[27] From draft 2013 DOT&E annual report: over 400 cybersecurity vulnerabilities were uncovered during the vulnerability assessment and/or the penetration testing that occurred during the operational test period. Of those, approximately half were serious (Category 1) vulnerabilities that could allow debilitating compromise to a system, and approximately three-quarters of the systems reviewed had one or more serious vulnerabilities. The three most common Category 1 vulnerabilities were: (1) out-of-date/unpatched software, (2) configurations that included known code vulnerabilities, and (3) the use of default passwords in fielded systems. All of the problem discoveries could have and should have been identified prior to operational testing.

The AO may grant an ATO for up to 3 years, at which time the system must be reauthorized. Reauthorization may also be required at any time during this three-year period, due to the results of an annual review or a major change in the system's cybersecurity posture (i.e., an increase in risk). Risk assessments are necessary to determine if, and to what degree, the risk has increased due to changes in the system, its environment, or its operation. If risk has increased, the authorizing official must be consulted to determine if a new authorization decision is required.

There is an emerging DoD strategy for Information Security Continuous Monitoring (ISCM). Each DoD Component develops its respective ISCM implementation plan to align with the overarching DoD ISCM strategy. Similarly, programs develop and align their respective system-level ISCM strategies with the Component and DoD-level guidance.

ISCM becomes an enabler of continuous reauthorization, in that the effectiveness of security controls is automatically or manually monitored so that the authorizing official can be made aware of any significant changes to the cybersecurity posture of the system in its operating environment.

The system-level continuous monitoring strategy developed and refined throughout the lifecycle is implemented in P&D. In accordance with this strategy, the system is monitored for cybersecurity-relevant events and configuration changes, the quality of security control implementation is periodically assessed, and significant changes in the system's cybersecurity posture are reported to the Security Control Assessor (SCA) and authorizing official.

The PM ensures the security plan and POA&M are updated based on the results of the system-level continuous monitoring process. The ISSM may recommend changes or improvements to the implementation of assigned security controls, the assignment of additional security controls, or changes or improvements to the design of the system itself to the SCA and AO at any time.

Continuous monitoring is performed at a system-level, but the information can be rolled up to provide an enterprise view. Mission owners and operators participate in continuous monitoring to ensure the effectiveness of security controls and in many cases provide input to PMs on the more technical security controls (i.e., controls applied to or by the system itself). PMs may be aware of and correct known system-level weaknesses, but computer network defense service providers can also advise information system owners and PMs of broader-based attacks and can offer evidence of and advice on exploitable vulnerabilities in the system that must be corrected or mitigated to protect the individual system, other systems on the enterprise network, and the enterprise network itself from exploitation.

IOT&E is conducted within a realistic threat environment based on the program's STAR. The PM coordinates with the designated Operational Test Agency (OTA) to ensure adequate

---

[28] For guidance on interoperability testing and certification, see DoDI 8330.01, Interoperability of IT and NSS, 21 May 2014, and the current version of the Joint Interoperability Test Command Interoperability (JITC) Process Guide (IPG).

[29] For details, see the Defense Information Systems Network (DISN) Connection Process Guide (CPG), which can be found at http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide.

cybersecurity activities are included in the operational test plans. Independent cybersecurity teams perform vulnerability assessments and penetration testing to assess, protect, detect, react to, and restore attributes of the system under test. A cybersecurity risk assessment is necessary to determine if any identified vulnerabilities can be exploited.[30] If any cybersecurity issues are identified, alternative courses of remediation to resolve identified issues, problems, root cause of failure, erroneous behavior, or other non-compliance issues are presented to the PM and authorizing official.

The MDA assesses the results of initial OT&E, initial manufacturing, and initial deployment, and determines whether or not to approve proceeding to Full-Rate Production or Full Deployment. If new validated threats or vulnerabilities are identified, and a cybersecurity risk assessment determines that they create deficiencies that may affect operational effectiveness, they will be identified in the POA&M.

A successful Full Rate Production (FRP) decision review indicates the manufacturing processes are mature and the capability has been successfully demonstrated through OT&E in a realistic operational environment. The FRP decision review confirms that an updated TSN analysis has been completed, an ATO has been granted, and the updated PPP has been submitted and approved.

A.4.2 Operations and Support: Monitor Cybersecurity and Risk after Authorization to Operate to Maintain Security Posture until Disposal

The purpose of the Operations and Support (O&S) phase is to execute the product support strategy, satisfy materiel readiness and operational support performance requirements, and sustain the system[31] over its lifecycle. O&S begins after the FRP or Full Deployment decision and is based on an MDA-approved Lifecycle Support Plan (LCSP).[32]

After the system is approved and fielded for operational use, the effectiveness of the program's cybersecurity capabilities is monitored in accordance with the system-level continuous monitoring strategy. Any change to the system, its environment, or its use has the potential to increase or decrease risk; therefore, a cybersecurity risk assessment is necessary to determine the risk level associated with changes.[33] Results of continuous monitoring and subsequent

[30] The most appropriate risk assessment approach depends on the level of detailed information provided by the vulnerability assessment and/or the penetration test. More details allow a more quantitative approach. Also, the most appropriate analytic approach at this point is a vulnerability-oriented approach, as the focus is on vulnerabilities that may be exploited by threat sources, while also understanding the impact to operations.

[31] The following are examples of O&S cybersecurity activities: implementing continuous monitoring; analyzing and implementing Information Assurance Vulnerability Alerts (IAVAs); applying patches as needed; maintaining and updating anti-virus/Host Intrusion Detection System (HIDS) signatures; maintaining local site infrastructure, facility, physical, and procedural cybersecurity requirements; and meeting reauthorization requirements.

[32] Annex E provides more information on cybersecurity lifecycle considerations.

[33] The risk assessment approach can vary, depending on the level of detailed information gathered during continuous monitoring. The more detailed the information, the more the approach can move from qualitative to semi-quantitative or quantitative. Also, the analytic approach can vary depending on the nature of the changes to the system. If new vulnerabilities are identified, the approach may be vulnerability oriented. If new threats are identified, the approach may be threat oriented. If it is necessary to primarily identify the impact to assets, an

cybersecurity risk assessments may necessitate changes to the system to mitigate newly identified and unacceptable risk; therefore, the PM updates the Security Plan and indicates in the POA&M how and when those changes will be implemented. The PM may need to coordinate with organizations outside the PMO to ensure actions identified in the POA&M are feasible and are ultimately implemented to the satisfaction of the authorizing official.

In addition to evaluating any changes to the system, the PM must maintain compliance with the DoD Vulnerability Management (VM) policy and all the VM reporting requirements. Non-compliance with the DoD VM policy may also affect authorization.

Cybersecurity considerations also apply to disposal,[34] which is the process of reusing, transferring, donating, selling, destroying, or otherwise disposing of excess surplus property. During the disposal phase of the system development lifecycle, the RMF requires organizations to implement an information system decommissioning strategy, which executes required actions when a system is removed from service. The strategy for disposal includes the communication approach and the management of risks associated with information system removal, decommissioning (e.g., media sanitization, configuration management and control, and security controls inheritance relationships), and destruction.[35] A cybersecurity risk assessment for decommissioned systems is conducted to identify the level of risk associated with decommissioning activities. The results of the risk assessment drive decisions on the appropriate steps taken to, at a minimum, ensure residual classified, sensitive, or privacy information is not exposed.

Refer to Annex E for detailed information of cybersecurity-related activities that occur during sustainment.

---

asset/impact-oriented approach may be used. Note also that a combination of approaches may be necessary, as determined by consulting the authorizing official and/or the SCA.

[34] A concept known as demilitarization (DEMIL) may take place during this phase. See DAG, Chapter 4, Section 4.3.18.7 Demilitarization and Disposal. DEMIL renders safe and eliminates functional capabilities and inherent military design features from both serviceable and unserviceable DoD materiel. It is the act of destroying the military offensive or defensive advantages inherent in certain types of equipment or material.

[35] *DoD 4140.1-R, Supply Chain Materiel Management Regulation*, and *DoD 4160.21-M, Defense Materiel Disposition Manual.*

Annex B - Cybersecurity Roles and Responsibilities

Annex B includes two key components:

1) A description of risk management framework (RMF)/cybersecurity stakeholder roles and responsibilities. In cases where the term for the role has changed from the term used under the DIACAP, the DIACAP term is noted.
2) A Responsible, Accountable, Supportive, Consulted, and Informed (RASCI) responsibility assignment matrix capturing major activities across the lifecycle, and how key stakeholders work together to integrate cybersecurity into the acquisition lifecycle.

PMs need to work with others in the cybersecurity community to develop and deliver secure systems and obtain timely and cost-effective system authorizations for their programs. Implementing cybersecurity requires cooperation and collaboration within the acquisition community and among many external stakeholders. The cybersecurity-specific roles and responsibilities of the stakeholders are described below:

- Authorizing Official (AO)
  - Responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture. (*Reference: DoDI 8510.01*)
  - DIACAP term: Designated Accrediting Authority (DAA)
- Chief Developmental Tester
  - Responsible for coordinating the planning, management, and oversight of all DT&E activities for the program; maintaining insight into contractor activities and overseeing the T&E activities; and helping PMs make technically informed, objective judgments about contractor DT&E results (*Reference: 10 US Code 139b)*
- Chief Engineer/Lead Systems Engineer
  - Acts as lead engineer for entire system; responsible for engineering analysis and trades made at the system level; works with system security engineer on integrating security into overall engineering efforts. (*Reference: DAG, Chapter 4*)
- Defense Intelligence Agency Threat Analysis Center
  - Utilizes intelligence and counterintelligence to assess risks that may be introduced intentionally or unintentionally by a particular supplier and provides standardized all-source intelligence assessments to inform program management and support acquisition risk management efforts. (*Reference: DAG, Chapter 13*)
- Developer
  - Role may be performed in-house, by another government entity, or by a contractor/system integrator. The developer should understand relevant threats and be able to assess mission needs and capability gaps against likely adversary threat capabilities. Development will be conducted in accordance with security

controls related to assurance, system development, and security best practices to reduce vulnerabilities and to design, build, and test security in the system early and cost effectively. (*Reference: DoDI 5000.02*)

- DoD Component Chief Information Officer (CIO)
    - Responsible for administration of the RMF within the DoD Component cybersecurity program; participation in the RMF Technical Advisory Group (TAG) visibility and sharing of the RMF status of assigned information system (IS) and PIT systems; and enforcement of training requirements for persons participating in the RMF. (*Reference: DoDI 8510.01*)
- Information Owner (IO)
    - Acts as statutory or operational authority for specified information; responsible for establishing the controls for data generation, classification, collection, processing, dissemination, and disposal. (*Reference: DoDI 8510.01/CNSSI 4009*)
- Information System Security Officer (ISSO)
    - Responsible for maintaining the appropriate operational security posture for an information system or program. (*Reference: DoDI 8510.01/CNSSI 4009*)
    - DIACAP term: Information Assurance Officer
- Information System Security Manager (ISSM)
    - Responsible for ensuring all products, services, and PIT have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system. (*Reference: DoDI 8510.01*)
    - DIACAP term: Information Assurance Manager
- Joint Staff's Functional Capability Board (FCB)
    - DoD body that is responsible for the organization, analysis, and prioritization of joint warfighting capabilities within an assigned functional area. (*Reference: JCIDS Manual*)
- Joint Requirements Oversight Council (JROC)/DoD Component Requirements Authority
    - Identifies and assesses the priority of joint military requirements to meet the national military and defense strategies, and considers alternatives to any acquisition program that has been identified to meet military capabilities by evaluating the cost, schedule, and performance criteria of the program and of the identified alternatives. (*Reference: CJCSI 5123.01*)
- Milestone Decision Authority
    - Sole and final decision authority. Approves entry of an acquisition program into each phase of the acquisition process and ensures programs are structured and resourced to succeed. (*Reference: DoDD 5000.01/DoDI 5000.02*)

- Operational Test Agency
    - Conducts a comprehensive cybersecurity vulnerability assessment in an operational environment to determine readiness for the Cyber Operational Resiliency Evaluation. (*Reference: DoDD 5141.02*)
- Program Executive Office
    - Responsible for executive management of assigned programs. Supervises design of acquisition programs, preparation of programs for decisions, and execution of approved program plans. (*Reference: DoDI 5000.02*)
- Program Manager /System Manager
    - Responsible for ensuring the program meets statutory and regulatory requirements for cybersecurity and for incorporating cybersecurity requirements into the program from conceptual development through design and sustainment/disposal. *(Reference: DoDI 5000.02)*
- Requirements Sponsor
    - Responsible for all capability requirements documentation (ICD, CDDs, CPDs, and Joint DOTmLPF-P Change Recommendations [Joint DCRs]), periodic reporting, and funding actions required to support the capabilities development and acquisition process for a specific capability proposal. (*Reference: CJCSI 3170H)*
- Security Control Assessor
    - Develops the Security Assessment Plan and ensures decomposed component security specifications, including verification criteria, are fully defined and traced to the controls delineated in the Security Plan. (*Reference: DoDI 8510.01)*
    - DIACAP term: Certifying Authority
- Systems Security Engineering
    - Provides the expertise needed to effectively integrate security, including cybersecurity, into the design and development of the system throughout the acquisition lifecycle. (*Reference: Defense Acquisition Guidebook*)
- User Representative
    - Defines the system's operational and functional requirements, and is responsible for ensuring that user operational interests are met throughout the system's authorization process. (*Reference: DoDI 8510.01/CNSSI 4009)*

Table 1 defines the meanings for R, A, S, C, and I in the RASCI table. The person or functional role is identified as Responsible, Accountable, Supportive, Consulted, and/or Informed for each activity or product. Table 2 provides acronyms for the RASCI roles. Table 3, the RASCI matrix, describes the roles and responsibilities for conducting or producing cybersecurity-related activities, products, and artifacts through each phase of the DoD acquisition lifecycle.

Table 1. Meanings for RASCI Matrix

RASCI Key	
Responsible	Role that executes one or more process activities. There may be multiple "R" roles for a process activity; however, there must be at least one.
Accountable	Role ultimately accountable for the work. Individual with final decision authority, or depending on the product, signatory authority.
Supportive	Role that is allocated to those who help to complete the task.
Consulted	Role that needs to be consulted before a final decision can be rendered. Two-way communication is assumed.
Informed	Role that is informed when a decision is made or an action is taken. One-way communication is assumed.

Table 2. Acronyms for RASCI Roles

RASCI Roles Abbreviations Key	
PM	Program Manager / System Manager
IO	Information Owner
SCA	Security Control Assessor
CE	Chief Engineer / Lead Systems Engineer
AO	Authorizing Official or Designated Representative
ISSM	Information System Security Manager or Information System Security Officer
UR	User Representative
D/SI	Developer or System Integrator
CDT	Chief Developmental Tester
OTA	Operational Test Agency
Intel	Defense Intelligence Agency or Component Intelligence Activity
Sponsor	Requirements Sponsor, Functional Sponsor, or Mission Owner
JROC	Joint Requirements Oversight Council or Component Requirements Authority
MDA	Milestone Decision Authority
CIO	DoD CIO or Component CIO
SSE	Systems Security Engineering (sometimes called Information System Security Engineering or Information Assurance System Engineering)
JS	Joint Staff

Note: These are not standard acronyms and should only be referenced for use with the RASCI matrix in this guidebook.

Cybersecurity-related activities, products, and artifacts as well as technical reviews, milestones, and decision points are presented for each phase of the acquisition lifecycle. Because individual program structures may be tailored, not every activity in the matrix is required for every program. The RASCI matrix should not be thought of as a compliance checklist to achieve cybersecurity integration. Instead, it summarizes how and when key stakeholders work together to integrate cybersecurity into the acquisition lifecycle.

Table 3. RASCI Matrix for the DoD Acquisition Lifecycle

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text**	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Acquisition Phase: Materiel Solution Analysis (MSA)																			
Materiel Development Decision (MDD)	R													A			R		DoDI 5000.02
Appoint an Information Systems Security Manager (ISSM) and ensure qualified system security engineer(s)	R A			C	C											I		Depending on the size of the program, a dedicated system security engineer may not be required. Optionally, the National Security Agency (NSA) may provide SSE support	DoDI 8510.01 - Enclosure 4
Categorize the system (identify potential impact levels due to the loss of confidentiality, integrity, and availability) to support Initial Capabilities Document (ICD) development Input to: **ICD** and **Security Plan**	R	R			A	R	C					R				C			DoDI 8510.01 - Enclosure 4

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Assess cybersecurity risk per criteria in Analysis of Alternatives (AoA) study plan and cybersecurity capability requirements from the ICD Input to: **AoA Study Plan**	S					R					S	A				R	C	Typically performed by study director	DoDI 5000.02
Determine preferred solution considering cybersecurity risks	S			S	C	S	C					R	C	A	C	S	R		DoDI 5000.02 - Enclosure 9
Develop initial **Security Plan**	A					R	C									C			
Select security control baseline including overlays Input to: **Security Plan**	R	I	I	C	A	R	C	C				S				R			DoDI 8510.01 - Enclosure 6
Ensure that initial security controls baseline traces to the preliminary system performance specifications that comprise the preliminary functional baseline	A			R	C	C	C									R			DoDI 8510.01 - Enclosure 6

Activity System Engineering Technical Review Milestone/Decision Review JCIDS/Requirements Review T&E ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Conduct Trusted Systems and Networks (TSN) Analysis focused at mission level, including Criticality Analysis (CA) to identify critical functions, Threat Assessment (TA), Vulnerability Assessment (VA), TSN Risk Assessment, and countermeasure selection Input to: **PPP**	A		C	R	C	C					S	C				R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the AO and SCA is encouraged during these steps, but may not always be practical due to resource limitations.	DoDI 5200.44 DoDI 5000.02 - Enclosure 11
Conduct cybersecurity risk assessment using the mission context as described in the ICD with consideration of likelihood of attack, as well as results from the TSN Risk Assessment Input to: **Security Plan**	A		C	R	C	R					S					C		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the AO and SCA is encouraged during these steps, but may not always be practical due to resource limitations.	DoDI 8510.01 - Enclosure 6
Alternative Systems Review (ASR) (best practice but not required)	A			R	I	C	C		C							R		AO informed by ISSM	
Functional Capability Board (FCB) review of AoA	S			C	I		C					R	A	I			R	AO informed by ISSM; JROC provides informed	CJCSI 3170.01H,

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
																		advice to the MDA	JCIDS, and JCIDS Manual
Identify applicable cybersecurity enterprise architectures in the system conceptual design	A	C		R		R	R					R			R	R	C		DoDI 8500.01 Enclosure 3 and 6 DoDI 5000.02 Enclosure 11 and 12
Incorporate final system categorization in the Draft Capability Development Document (CDD) Input to: **Draft CDD**	C					S						A	R		R		C		DoDI 8510.01 - Enclosure 6
Develop the initial Cybersecurity Strategy. Append to the Program Protection Plan (PPP) Input to: **Cybersecurity Strategy**	R			C	C	R					S	S			A	R			DoDI 8510.01 - Enclosure 6 DoDI 5000.02 - Enclosure 11
Document the cybersecurity capability requirements and planned security controls to meet those requirements	R	I	I	C	A	R	C	C				S				R			DoDI 8510.01 - Enclosure 6

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **Security Plan**																			
Develop the system-level continuous monitoring strategy Input to: **Continuous Monitoring Strategy**	R		S		A	S									R	S			DoDI 8510.01 - Enclosure 6
Milestone A	R													A			R		DoDI 5000.02
Acquisition Phase: Technology Maturation & Risk Reduction (TMRR)																			
Refine derived cybersecurity system-level requirements. Provides input to the System Requirements Review (SRR)	A			R		C	C	I	C			C				R			
Refine and coordinate the derived cybersecurity requirements among the system's PPP, Cybersecurity Strategy, Security Plan, and specifications for the technical solution in preparation for the SRR	A			R	I	R	C	C	C			C				R			DoDI 8510.01 - Enclosure 6

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text**	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **PPP, Cybersecurity Strategy,** and **Security Plan**																			
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection Input to: **Security Plan**	A		C	R	C	C		C			S	C				R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the AO and SCA is encouraged during these steps, but may not always be practical due to resource limitations.	DoDI 5200.44 DoDI 5000.02 - Enclosure 11
Update cybersecurity risk assessment (includes Threat, Vulnerability, Likelihood, and Impact), including results from the TSN analysis Input to: **PPP**	A		C	R	C	R					S					R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the AO and SCA is encouraged during these steps, but may not always be practical due to resource limitations.	DoDI 8510.01 - Enclosure 6
SRR					I	C	C		C									AO informed by ISSM	

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
	A			R				S								R			
Refine the system specifications by translating and deriving cybersecurity specifications from the system's cybersecurity capability requirements (both explicitly specified and implicitly derived) Input to: **EMD RFP**	A			R		C	C	S	S			C				R			DoDI 8510.01 - Enclosure 6
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection Input to: **PPP**	A		C	R	C	C		C			S	C				R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the AO and SCA is encouraged during these steps, but may not always be practical due to resource limitations.	DoDI 5200.44 DoDI 5000.02 - Enclosure 11
Acquisition Phase: Technology Maturation & Risk Reduction (TMRR)																			

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text**	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Evaluate that the system functional baseline satisfies the draft CDD's cybersecurity requirements; that functional requirements and verification methods support achievement of performance requirements in the System Functional Review (SFR); and that functional requirements and verification methods support the initial Engineering & Manufacturing Development (EMD) Request for Proposal (RFP) development Input to: **EMD RFP**	A			R		C	C	S	C			C				R			DoDI 8510.01 - Enclosures 4 and 6
SFR	A			R	I	C	C	S	C							R		AO informed by ISSM	
Align the Test and Evaluation Master Plan (TEMP) with the Security Assessment Plan, Systems Engineering Plan (SEP), PPP, Cybersecurity Strategy, STAR, and Acquisition Strategy	A		C	C					R	C						C			DoDI 5000.02 - Enclosure 5

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **TEMP**																			
Develop the Security Assessment Plan. The SAP should be aligned with the TEMP, SEP, PPP, Cybersecurity Strategy, and Acquisition Strategy Input to: **SAP**	C		R	C	A	C			C							C			
Update the SEP and PPP. Align with the TEMP, SAP, and Acquisition Strategy Input to: **SEP** and **PPP**	A			R				C	C							C			DoDI 5000.02 - Enclosure 3
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection	A		C	R	C	C		C			S	C				R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the AO and SCA is encouraged during these	DoDI 5200.44 DoDI 5000.02 - Enclosure 11

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **PPP**																		steps, but may not always be practical due to resource limitations.	
Develop the EMD RFP and update the Acquisition Strategy. Align with the TEMP, SAP, and SEP Input to: **EMD RFP** and **Acquisition Strategy**	A R			C					C										DoDI 5000.02
Development RFP Release Decision Point	R			C	I	C			C	C		C		A	C	C	C	AO informed by ISSM	DoDI 5000.02
Define the allocated baseline (including cybersecurity considerations) Input for: **Preliminary Design Review (PDR)**	A		C	R	C	C	C	C	R				C			R			DoDI 5000.02 - Enclosure 3
PDR	A		C	R	I	C	C	S	C							R		AO informed by ISSM	
Milestone B	R													A			R		DoDI 5000.02

Activity System Engineering Technical Review Milestone/Decision Review JCIDS/Requirements Review T&E ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Acquisition Phase: Engineering & Manufacturing Development (EMD)																			
Map and allocate cybersecurity requirements to the hardware and software design for the system as part of the overall system development process and to support test and evaluation planning	A			R		C		C	I							R			DoDI 5000.02
Characterize the attack surface and begin to assess cybersecurity in planning and performing component and system integration testing	A			R		C		R	R	C						C			
Complete the detailed build-to design of the system, ensuring that cybersecurity requirements are included				C				R								C			DoDI 5000.02
Conduct systems engineering, including technical planning as defined in the approved SEP, and verify compliance with the functional, allocated, and product baselines				A				R	I							R			DoDI 5000.02 - Enclosure 3

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Ensure that cybersecurity requirements are mapped and allocated to the hardware and software design				R				R								R			
Ensure that Critical Design Review (CDR) entrance criteria for cybersecurity baseline design are met and that all cybersecurity requirements are reflected in the product baseline, which includes the design Input for: **CDR**	A			R		C		C	C							R			
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection Input to: **PPP**	A		C	R	C	C		C			S					R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the SCA and AO is encouraged during these steps, but may not always be practical due to resource limitations	DoDI 5200.44 DoDI 5000.02 - Enclosure 11

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Update cybersecurity risk assessment (includes Threat, Vulnerability, Likelihood, and Impact), including relevant results from TSN analysis Input to: **Security Plan**	R		C	R	C	A			I		S					R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the SCA and AO is encouraged during these steps, but may not always be practical due to resource limitations	DoDI 8510.01 - Enclosure 6 DoDI 5200.44 DoDI 5000.02 - Enclosure 11
CDR	A		C	R	C	C	C	S	C							R			
Develop Security Assessment Plan (SAP) in support of the Interim Authorization To Test (IATT) application. Provide to the Authorizing Official Input to: **SAP**			R	C	A	I		S	C							C			DoDI 8510.01 - Enclosure 6

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Assess the system using appropriate procedures to determine the extent to which the controls are effective, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Prepare a Security Assessment Report (SAR) against the Security Assessment Plan Input to: **SAR**			R					I	I							C			DoDI 8510.01 - Enclosure 6
Submit draft Security Authorization Package at IATT in order to conduct system testing activities	R				A	R		S	C							I			DoDI 8510.01 - Enclosure 6
Conduct vulnerability analysis and testing to evaluate the system's cybersecurity in a mission context using realistic threat exploitation techniques			C	C	C			I	R	C						C			DoDI 5000.02 - Enclosure 4

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Conduct developmental test and evaluation (DT&E) event to demonstrate system maturity and readiness to begin production and preparedness for operational test and evaluation and/or deployment and sustainment activities			C	C		I		S	R							C			DoDI 8510.01 - Enclosure 6
Prepare DT&E assessment as input to Milestone C Decision Input to: **DT&E Assessment**			C	C				S	R	C						C			DoDI 5000.02 - Enclosure 4
Conduct Vulnerability and Penetration Assessment that includes overt, cooperative, and comprehensive examination of the system to characterize the system's operational cybersecurity status. Input for: **Functional Configuration Audit**			C	C				I	C	R									DoDI 8510.01 - Enclosure 6

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text**	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Implement and verify cybersecurity-derived requirements in the hardware and software design for transition to the development and manufacturing environment Input for: **Functional Configuration Audit**				R		C										R			
Functional Configuration Audit	A			R		C		S								R			
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection Input to: **PPP**	A		C	R	C	C		C			S					R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the SCA and AO is encouraged during these steps, but may not always be practical due to resource limitations	DoDI 5200.44 DoDI 5000.02 - Enclosure 11
System Verification Review	A			R		C		S								R			
Production Readiness Review																			

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
	A			R				S								R			
Milestone C	R													A			R		DoDI 5000.02
Acquisition Phase: Production and Deployment (P&D)																			
Submit complete Security Authorization Package to obtain Authorization To Operate (ATO) decision	A					R		S	C							C			DoDI 8510.01 - Enclosure 6
Issue the ATO decision	I		I		A	I	I	I	I						I	I			DoDI 8510.01 - Enclosure 6
Submit network connection approval package	A	I	I		I										I			Approval authority is based on the network.	DoDI 8510.01 - Enclosure 3
Assess cybersecurity during initial operational test and evaluation (IOT&E)	I		I	C		I			C	A R		I				C			DoDI 5000.02 - Enclosure 5
Conduct an adversarial IOT&E on low-rate initial production systems that supports full fielding decisions	I		I	C		I		I	C	A R		I							DoDI 5000.02 - Enclosure 5
Update the SAR, incorporating the OT&E data			A R		I	I										I		Different entities may fulfill the SCA role throughout the lifecycle of	DoDI 8510.01 - Enclosure 6

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **SAR**																		the program	
Update cybersecurity risk assessment for deficiencies/weaknesses Input to: **Security Plan**	I	I	A R	C		C		S			S					R		Different entities may fulfill the SCA role throughout the lifecycle of the program	
Based on results of the cybersecurity risk assessment, document corrective actions in the Risk Management Framework (RMF) Plan of Action and Milestones (POA&M) **Input to: RMF POA&M**	A	I	C	C	C	R		S	C			I				C			DoDI 8510.01 - Enclosure 6
If cybersecurity risk increases after IOT&E, provide the AO with an updated risk assessment to determine if a new ATO is necessary	I		R		A	C					S					R			DoDI 8510.01 - Enclosure 6
Address any deficiencies prior to the Full-Rate Production or Full Deployment decision	A				C	R						C				C			

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **Security Plan**																			
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection Input to: **PPP**	A		C	R	C	C		C			S					R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the SCA and AO is encouraged during these steps, but may not always be practical due to resource limitations	DoDI 5200.44 DoDI 5000.02 - Enclosure 11
Approve the updated Security Plan	I			I	A	I						I							
Address deficiencies prior to the Full-Rate Production or Full Deployment decision Input to: **PPP**				R				C	I					A		R			DoDI 5000.02 - Enclosure 3
Update the cybersecurity strategy to address the deficiencies prior to the Full-Rate Production or Full Deployment decision	R			C	C	R						S			A	R			

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Input to: **Cybersecurity Strategy**																			
Include cybersecurity activities in Lifecycle Sustainment Plan (LCSP) Input to: **LCSP**	R			C		C								A		C			DoDI 5000.02 - Enclosure 6
Physical Configuration Audit (PCA)	A			R		C		S								R			
Full-Rate Production or Full Deployment Decision	R													A			R		DoDI 5000.02
Acquisition Phase: Operations and Support (O&S)																			
Implement the system-level Continuous Monitoring Plan developed in MSA	A	S	C	C	C	R	C									C			DoDI 8510.01 - Enclosure 6
Based on evolving cybersecurity threats and required corrective actions, update the LCSP, Security Plan, POA&M, PPP, and Cybersecurity Strategy while	A	C	C	C	C	R	C									C			DoDI 5000.02 - Enclosure 6

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text***	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
the program is in sustainment Input to: **LCSP, Security Plan, POA&M, PPP,** and **Cybersecurity Strategy**																			
Throughout sustainment, conduct cybersecurity activities as needed, including: ▪ Implement Information Assurance Vulnerability Alerts (IAVAs) ▪ Apply software patches and updates ▪ Update and maintain anti-virus/HIDS signatures ▪ Apply Warning Orders and Operation Orders ▪ Update or replace hardware ▪ Apply firmware updates ▪ Perform reauthorization as needed per the DoD RMF for IT requirements ▪ Maintain local site infrastructure, facility, physical, and procedural security requirements	I	I	I	C	C	R	C					R				R		Sponsor (Mission Owner) includes users and operators	

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text**	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection Input to: **PPP**	A		C	R	C	C		C			S					R		The results of the TSN analysis will often impact the implementation of cybersecurity in the system. Coordination with the SCA and AO is encouraged during these steps, but may not always be practical due to resource limitations	DoDI 5200.44 DoDI 5000.02 - Enclosure 11
Update cybersecurity risk assessment (includes Threat, Vulnerability, Likelihood, and Impact). Provides input to the **Security Plan**	A	I	C	R	C	C	I	S	C		S					R			
In-Service Review (ISR) (Additional ISRs during O&S until decommissioning are typically critical for systems that change frequently, such as commercial-off-the-shelf and software-intensive systems)	A			R	C	R	C			S						R			

Activity **System Engineering** **Technical Review** **Milestone/Decision Review** **JCIDS/Requirements Review** **T&E** ***Artifacts or Products informed by activities shown in bold text**	**PM**	**IO**	**SCA**	**CE**	**AO**	**ISSM**	**UR**	**D/SI**	**CDT**	**OTA**	**Intel (e.g. DIA)**	**Sponsor**	**JROC**	**MDA**	**C I O**	**SSE**	**JS**	**Notes**	**Reference(s)**
After sustainment, implement disposal phase. A risk assessment for decommissioned systems should be conducted and the appropriate steps taken to ensure that residual classified, sensitive, or privacy information is not exposed.	A	I	C	R	I	C	I	S	C							R			DoDI 5000.02 - Enclosure 6
For systems inheriting controls from a decommissioned system, ensure that "disinherited" controls are implemented elsewhere	I	I	C	C	I	R	I												DoDI 8510.01 - Enclosures 4 and 6

Annex C - Cybersecurity Engineering Considerations

C.1 Introduction

This annex discusses key cybersecurity topics and activities as they relate to systems engineering for DoD acquisition programs. As explained in DoDI 5000.02, "Systems engineering provides the integrating technical processes and design leadership to define and balance system performance, life-cycle cost, schedule, risk, and system security within and across individual systems and programs. The Program Manager, with support from the Lead Systems Engineer, will embed systems engineering in program planning and execution to support the entire system life cycle."

The integration of cybersecurity into the systems engineering process is critical to planning for, designing, developing, deploying, and maintaining a system that is able to meet its operational capability requirements and is trustworthy and resilient in the face of a capable cyber adversary. Cybersecurity is integrated into systems engineering through systems security engineering (SSE). This annex is not intended to be a detailed guide for implementing SSE, but will highlight key topic areas and interactions among established processes to help PMs and their teams understand them.

C.2 Background

DoDI 5000.02 makes the program manager (PM) responsible for identifying and reducing technical, schedule, and cost risks to the program, and even renames an early stage of the acquisition lifecycle the Technology Maturation and Risk Reduction phase, although risk identification, reduction, and management activities occur in every other phase of the program as well. Many of the system engineering activities occurring throughout the lifecycle of a program are devoted to risk identification, reduction, and management. For DoD IT, see *DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT).* Focused on cybersecurity risk, DoDI 8510.01 explains that risk management should be initiated as early as possible and fully integrated into the DoD acquisition process, including requirements management, system engineering, and test and evaluation. Early integration of cybersecurity and RMF activities in acquisition processes reduces risk throughout the lifecycle, and minimizes the additional effort and cost required to achieve an authorization decision and the resources required to manage and monitor security controls throughout the system lifecycle. Early integration of cybersecurity requirements into a system/product/service lifecycle helps facilitate development and deployment of more resilient systems/products/services to reduce risk to mission operations and business functions.

The RMF for DoD IT is not intended to be implemented separately from the systems engineering process. This approach is integral to *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, which is the basis for the RMF for DoD IT. "Without the early integration of security requirements, significant expense may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design. When security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer

weaknesses and deficiencies, and therefore, less vulnerability that can be exploited in the future. Early integration of information security requirements into the system development lifecycle is the most cost-effective and efficient method for an organization to ensure that its protection strategy is implemented. It also ensures that information security processes are not isolated from the other routine management processes employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions and business functions. In addition to incorporating information security requirements into the system development lifecycle, security requirements are also integrated into the planning, programming, and budgeting activities within the organization to ensure that resources are available when needed and program/project milestones are completed."

Rather than carve out a stand-alone process for implementing cybersecurity, engineers should take a holistic approach to designing and developing a system that provides all the needed capabilities and fulfills all the stated and derived requirements and performance specifications, including cybersecurity. For example, cybersecurity functions, performance, and characteristics are incorporated into the system performance specifications, item performance specifications, item detail specifications, and the corresponding functional, allocated, and product baselines. Programs also need to develop solution architectures that incorporate system-level security and align with DoD Component and DoD enterprise security architectures. It is important for the program to engage their intelligence representative as early as possible for current and future threat information to understand the expected cyber threat environment in which the system will operate in order to understand and detail the operational and mission requirements and flow requirements down to system performance specifications, and detailed acquisition, engineering, and early DT&E strategies.

C.3 Roles and Responsibilities

Because every program is designed to address a unique set of capability requirements, PMs are allowed flexibility to structure, tailor, and phase their approach to reflect the needs and circumstances of the system they are developing and acquiring. These characteristics may include the complexity of the system, the need to account for certain identified threats or other risk factors, and the expected amount of time needed to develop and produce a system that satisfies the validated capability requirements. The same is true for the application and integration of cybersecurity into the systems engineering process.

To ensure security is designed into the system in the most cost-efficient manner, SSE is often integrated into systems engineering (SE) as a specialty discipline. SSE is "an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities," as defined in *DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).*

SSE is a process that captures and refines cybersecurity requirements and ensures these requirements are effectively integrated into the system and components through purposeful security architecting, design, development, and configuration. System security engineers are an integral part of the development team designing and developing new systems or upgrading legacy systems. System security engineers employ best practices when implementing security controls within a system, including software engineering methodologies, system/security

engineering principles, secure architecture, secure design, and secure coding techniques. SSE supports the development activities of programs and results in design-to and build-to specifications providing lifecycle protection for critical defense resources. SSE can be performed by a dedicated person or a variety of professionals with expertise in one or more areas, including SE, cybersecurity, security technologies, software assurance, vulnerability analysis, and hardware assurance. Typically, a system security engineer, or those performing these functions, will report to the lead engineer on the program. SSE leverages and adapts the principles and practices of SE within the same system lifecycle framework that governs SE processes. SSE activities are intended to secure the system by both "designing-in" the necessary countermeasures and "engineering-out" vulnerabilities throughout the lifecycle of the program.

The structure and size of the SSE organization should reflect the level of security required to counter the threats targeting the development environment of the system and of the system itself. The program's linkage between SE and SSE should be described in the program's SEP,[36] and include details on the respective roles, responsibilities, and relationships between the system engineer, the system security engineer, the SE Integrated Product Team (IPT), and SSE or Cybersecurity/Information Assurance IPT/sub-IPT. The ISSM normally chairs the Cybersecurity/Information Assurance IPT/sub-IPT. The PM selects the chairperson of the IPT/sub-IPT. The SEP should also discuss the SETR plan and processes, the entrance/exit and evaluation criteria for each SETR, expected products and deliverables, and the processes that will be used to incorporate engineering requirements and specifications into the program's RFP or other solicitation documentation.

Based on the resources available and the level of IT in the system, a PM may decide to augment the SE IPT with a dedicated system security engineer, ISSM, user representative, or other subject matter expert (SME) from a related information security or cybersecurity discipline. Tasks that could be assigned to these individuals would include oversight of or support to the RMF-related processes and documentation, including the Security Plan and Security Assessment Plan, which are worked in coordination with the SCA and authorizing official. The roles, responsibilities, and assignments of each member of the program management and engineering teams should be spelled out in the SEP and other program management documents that outline specific roles, responsibilities, and work assignments for all team members.

C.4 Cybersecurity Engineering References

A number of helpful resources are available to PMs and their teams that provide more detail on the topics discussed in this annex. The following references can be used to help programs understand additional requirements and related guidance for cybersecurity and systems security engineering for DoD systems.

[36] The SEP captures the program's current status and evolving SE process, plan, and implementation and its relationship to the overall program management effort. The plan documents key technical risks, processes, resources, metrics, SE products, and completed and scheduled SE activities, along with other program management and control efforts such as the Integrated Master Plan, Risk Management Plan, Technical Performance Measures, and other documentation fundamental to successful program execution. For more details on SEP requirements and processes, see the DAG, Chapter 4.

Defense Acquisition Guidebook (DAG), Chapter 4: Provides overarching guidance on the SE discipline, its activities and processes, and its practice in defense acquisition programs. (https://dag.dau.mil/Pages/Default.aspx)

DAG, Chapter 13: Provides overarching guidance on the SSE discipline and DoD program protection activities, processes, and practices for defense acquisition programs. (https://dag.dau.mil/Pages/Default.aspx)

DoD Risk Management Framework (RMF) Knowledge Service (KS): A dynamic online knowledge base supporting RMF implementation, planning, and execution by functioning as the authoritative source for RMF procedures and guidance. It supports RMF practitioners by providing access to DoD security control baselines, security control descriptions, security control overlays, and implementation guidance and assessment procedures. (https://rmfks.osd.mil)

DRAFT NIST SP 800-160, Systems Security Engineering: Describes how to implement the SSE processes in terms of the ISO 15288 processes. (http://csrc.nist.gov/publications/PubsSPs.html)

NIST SP 800-82, Industrial Control Systems Security Guide: Provides Supplemental and Enhanced guidance on the use of NIST SP 800-53 security controls when applied to ICS. (http://csrc.nist.gov/publications/PubsSPs.html)

Trusted Systems and Networks (TSN) Analysis Whitepaper: Intended to be used as an extension to guidance provided in DAG Chapter 13, Program Protection. It provides further details for TSN analysis processes, methods, and tools. It elaborates on each of the major iterative processes necessary to accomplish the TSN analysis objectives. (http://www.acq.osd.mil/se/docs/Trusted-Systems-and-Networks-TSN-Analysis.pdf)

Suggested Language to Incorporate Systems Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals: Intended for use by acquisition PMs who are preparing RFPs to help them implement *DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*. (http://www.acq.osd.mil/se/initiatives/init_pp-sse.html)

C.5 Program Protection Planning

The primary vehicle for integrating SSE activities into SE activities in the DoD is program protection planning. Program protection is the integrating process for managing risks to DoD warfighting capabilities from foreign intelligence collection; from hardware, software, vulnerability, or supply chain exploitation; and from battlefield loss throughout the system lifecycle. To mitigate these risks, a program seeks to protect technology, components, and information from compromise and unauthorized disclosure through the cost-effective application of countermeasures, documented in the PPP in accordance with DoDI 5000.02.

The two main analyses associated with the PPP are the TSN Analysis and the Critical Program Information (CPI) analysis. The PPP describes the program's CPI, mission-critical functions, critical components, the threats to and vulnerabilities of these items, the plan to apply countermeasures to mitigate associated risks, and planning for exportability and potential foreign

involvement. The PPP also discusses countermeasures to mitigate or remediate vulnerabilities throughout the system lifecycle, including design, development, developmental and operational testing, operations, sustainment, and disposal. Countermeasures may align to multiple security disciplines, including anti-tamper, exportability features, security (including cybersecurity, operations security, information security, personnel security, and physical security), secure system design, supply chain risk management, software assurance, anti-counterfeit practices, and procurement strategies. PMs may also incorporate automated software vulnerability analysis tools throughout the lifecycle, and ensure remediation of software vulnerabilities is addressed in PPPs, test plans, and contract requirements.

These processes are implemented across the full acquisition lifecycle to build security into the system. They are repeated at each SETR, during SE analyses in preparation for each acquisition milestone, in preparation for the RFP release, and at other points in the lifecycle, as needed. The PPP is submitted for MDA approval at each milestone and decision review, beginning with MS A, and is updated throughout the acquisition lifecycle.

The systems security engineer, working in concert with the Chief Systems Engineer, is usually responsible for developing and updating the PPP and presenting the corresponding analyses at each of the SETRs. The systems security engineer balances the security requirements among the different security disciplines to ensure a secure and affordable system can be developed.

DoDI 5000.02 and DoDI 8500.01 require the Cybersecurity Strategy to be documented and appended to the PPPs for all acquisition programs. DoDI 8500.01 also requires that the PPP review process and the review of other SE documents evaluate the status of cybersecurity solutions as part of the larger system development activities. In addition, cybersecurity is one of the key security disciplines required to be addressed as a countermeasure to TSN and CPI risk in the PPP.

DAG Chapters 4 and 13 offer more information on the respective roles, responsibilities, and relationships for SE, SSE, and program protection specialists, and explains how these activities should be integrated into the overall acquisition lifecycle planning and implementation activities.

C.6 TSN Analysis

In accordance with DoDI 5200.44, mission-critical functions and critical components must be protected and this protection can be accomplished through TSN analysis, one of the key Program Protection activities. Mission-critical functions are those functions of the system being acquired that, if corrupted or disabled, would likely lead to mission failure or degradation. Critical components are primarily the elements of the system (hardware, software, and firmware) that implement critical functions. In addition, the system components that implement protections of those inherently critical components (i.e., defensive measures), and other components with unmediated access to those inherently critical components, may themselves be mission critical.

Programs conduct a criticality analysis to identify their systems' mission-critical functions and components throughout the lifecycle and determine the appropriate countermeasures to apply to protect these items. The planning and execution activities include:

- Identification of the mission-critical functions and critical components of the system, commensurate with system requirements decomposition.
- Proactive TSN Key Practices planning and implementation.
- Assessment and analysis of threats, vulnerabilities, and risk for identified mission-critical functions and critical components.
- Trade-space and resource considerations.
- Risk mitigations and countermeasures planning and implementation.
- Risk identification after countermeasures are implemented, including follow-up mitigation plans and actions.

A program completes TSN analysis by performing Criticality Analysis (CA), Threat Assessment (TA), Vulnerability Assessment (VA), Risk Assessment (RA), and countermeasure selection and application. Figure 11 describes the relationships between these activities.

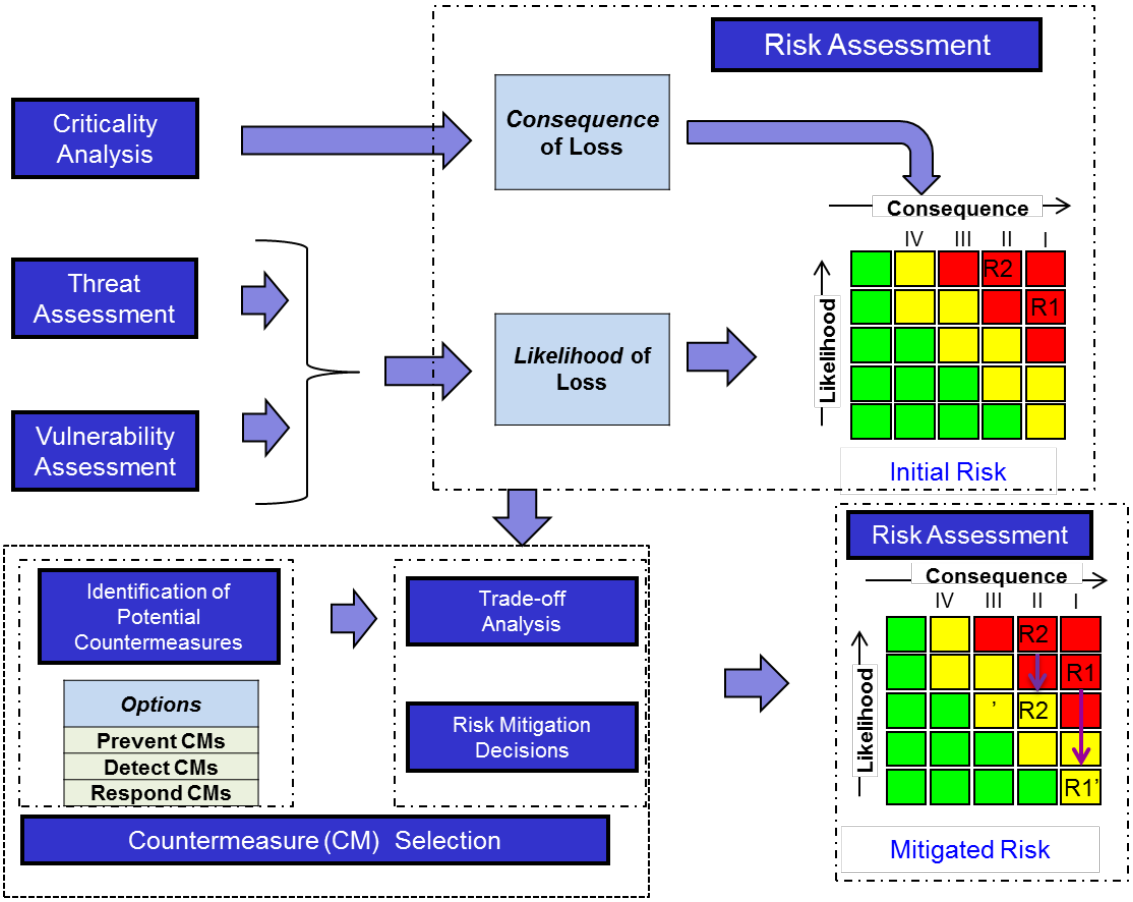


Figure 11. TSN Analysis

The TSN analysis process is applied throughout the acquisition lifecycle and should take into consideration system security risks for the program. As the system evolves, the program reconsiders the criticality of the functions and components as well as the vulnerabilities and threats. By periodically repeating the risk management process, the program may identify additional threats and vulnerabilities that were not identified in previous iterations because the level of detail of the design was not sufficient to identify them. This continuous risk

management with updated risks and countermeasures informs the system design trade-offs. Discovery of a potentially malicious source from the threat assessment may warrant additional checks for vulnerabilities in other (less critical) products procured from that source. For each program protection risk that is very high or high, a risk cube and mitigation plans are needed (see figure 11).

Efforts to identify mission-critical functions, critical components, and their protection begin early in the lifecycle and are revised as system designs evolve and mature. Cybersecurity risk assessment and TSN analysis activities and processes should inform one another to achieve a more cohesive and comprehensive cybersecurity risk picture. The analysis is updated at each of the technical reviews to take into account the latest design and implementation decisions as well as additional threat and vulnerability information. The level of detail required for TSN analysis as it progresses through the lifecycle should increase commensurate with system specification level. Many of the security controls implemented through the RMF align with the security specialty areas associated with TSN analysis. In these cases, controls may be implemented or tailored as countermeasures to TSN or system security risk, documented in the PPP.

C.7 Requirements Traceability and Security Controls

Requirements are identified initially as user-stated capabilities through the JCIDS process. These desired capabilities are decomposed and refined, then incorporated in combination with additional "stakeholder" defined requirements that include those specified in relevant policies and guidelines, and elicited through user and stakeholder interaction.

Baseline security control sets and DoD Component or domain-specified overlays identified via the RMF are selected and incorporated into these initial high-level requirements. Security controls are not initially articulated in requirements language, but are integrated into system design via SSE requirements analysis, decomposition, validation, verification and test, and configuration management in combination and context with all other requirements. An entry-level decomposition of security controls into requirements statements has been conducted via the Control Correlation Identifier (CCI) product, a standard identifier and description for each of the singular, actionable statements that comprise a security control or best practice. CCI bridges the gap between high-level policy expressions and low-level technical implementations. The CCI product set can be found at http://iase.disa.mil/stigs/cci.html.

Individual CCIs may be incorporated as appropriate into initial Statements of Work or Objectives, System Requirements Documents, Contract Data Requirements Lists (CDRLs), and Integrated Master Plans/Schedules (IMPs/IMSs), providing direct traceability between security controls and derived requirements and specifications that can be maintained throughout the development lifecycle. To ensure initial user, performance, and functional requirements are correctly translated into product specifications and the final design, the systems security engineer/ISSM should fully participate in IPT analyses, trades, configuration management, and risk deliberations, and throughout SETR processes and reviews.

During successive iterations of the requirements analysis and refinement processes, the set of security controls will be further tailored to determine if they sufficiently address system stakeholder or user requirements. Additional engineering trades (discussed below) will be conducted within the SSE space, as well as across all SE, in light of cost, schedule, and

performance impacts, and may result in additional controls tailoring and other mitigations. As the program continues to tailor the set of security controls, they are translated into requirements and design details to ensure they mitigate vulnerabilities and risks to confidentiality, integrity, and availability. The security requirements are captured in the capability requirements and functional, allocated, and product technical baselines to ensure they are implemented and traced throughout the design and development of the system. As Figure 12 shows, there should be direct traceability between the user-stated and derived requirements, specifications, security control sets, and tailored controls at all levels of abstraction.

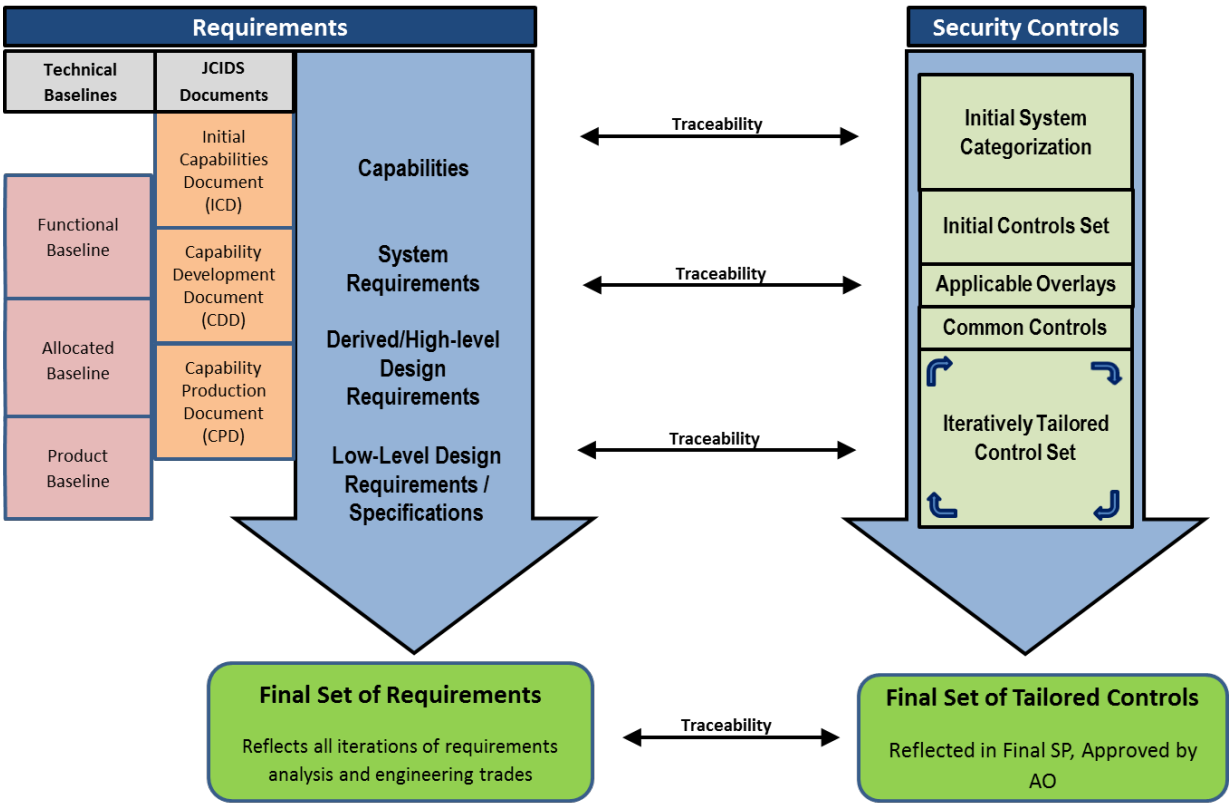


Figure 12. Traceability of Requirements to Controls

C.8 Selecting and Tailoring Security Controls

Figure 13 depicts the basic process of security control selection and tailoring, and how SSE interacts with the process.

Once the system is categorized, the next step is to identify the appropriate baseline security controls, apply any applicable overlays, and document this initial controls set in the Security Plan. Common controls that will be inherited are then identified. Programs should tailor the initial control set to account more closely for conditions affecting the specific system (i.e., conditions related to organizational missions/business functions, information systems, or environments of operation). See the RMF Knowledge Service, CNSSI 1253, and NIST SP 800-53 for more information on the selection and tailoring of security controls. All of the controls implemented are selected from NIST SP 800-53.

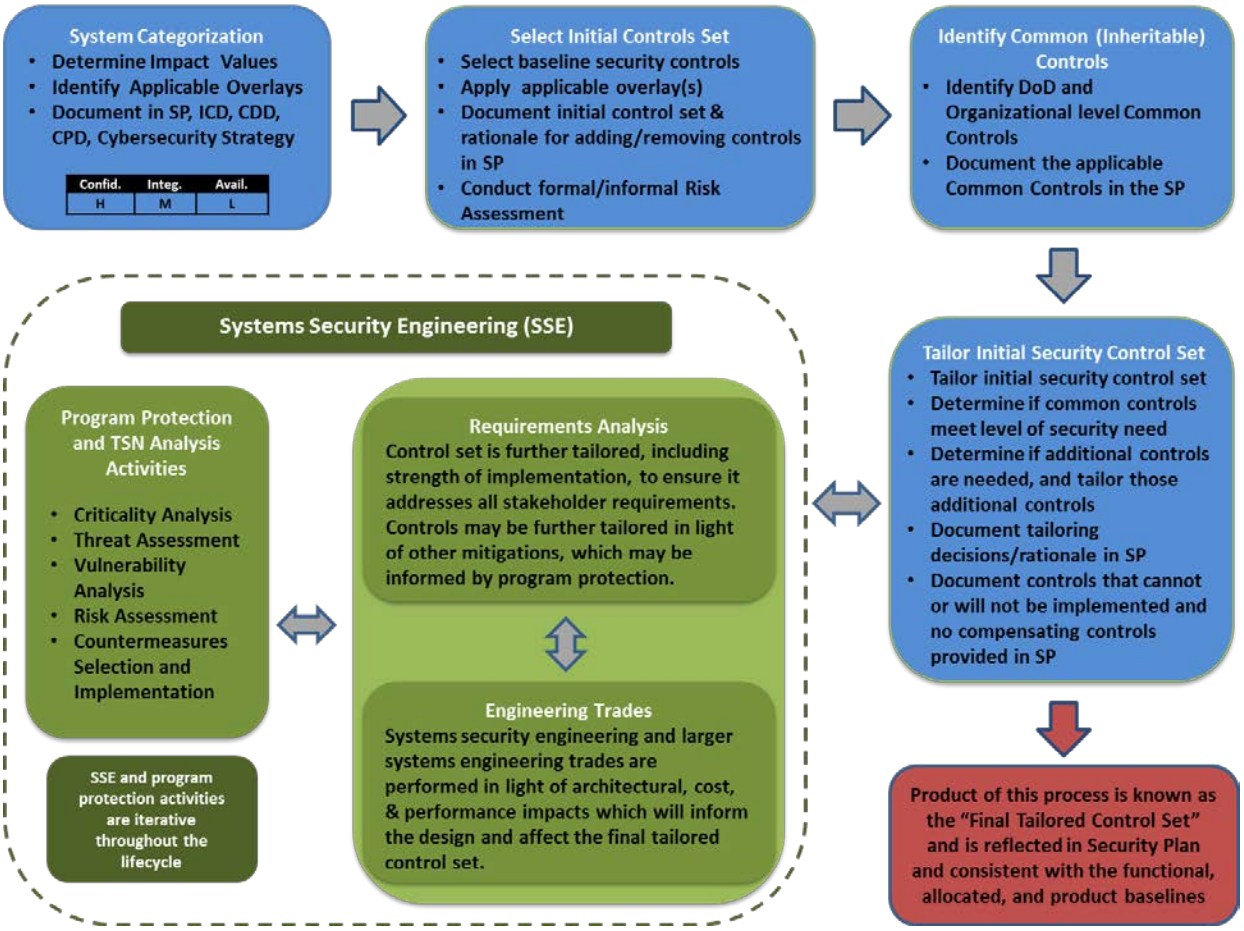


Figure 13. Security Control Selection and Tailoring Process

Table 4 depicts the 18 families of controls in NIST SP 800-53. The controls in these families may fall into a number of categories. Some controls are applied at the organization level, while some are applied to the system itself. Controls may be intended to protect, detect, react, or restore a system's capability. Controls can be technical in nature, focused on policy, apply to the development environment, apply to contracting, and be operational in nature. Some controls focus on improving resilience and some on attaining a higher level of assurance. Controls also may be applied differently depending on the system type (e.g., enclave or PIT system) or lifecycle phase. Although controls may be broken out and categorized in many ways, NIST SP 800-53 attempts to provide organizations with the breadth and depth of security controls necessary to fundamentally strengthen their systems and the environments in which those systems operate.

Table 4. Security Control Identifiers and Family Names

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

The product of this tailoring process is the initial tailored control set, because the tailoring of controls is an iterative process throughout the acquisition lifecycle that reflects requirements analysis and engineering trades after the preferred alternative is selected and the draft CDD is developed.

Programs should also document and justify in the Security Plan any security controls from the initial security control set that cannot or will not be implemented in the system and for which no compensating control(s) will be substituted. At the discretion of the AO, this information may be included in the Security Plan and the POA&M.

C.9 Engineering Trade Analyses

Throughout the acquisition lifecycle, the program will conduct a series of SE and SSE trade-off analyses to assess the system's affordability and technical feasibility to support requirements, budget/investment, and acquisition decisions. These analyses may also depict the relationships between system lifecycle cost and the system's performance requirements, design parameters, and delivery schedules. The results of these analyses should be reassessed over time as system requirements, design, manufacturing, test, and logistics activities evolve and mature. The iterative processes of performing requirements analyses and engineering trades can also be used to identify any security gaps and materiel/non-materiel approaches and trade-offs among the possible security requirements, and related controls to address those gaps.

Early integration of cybersecurity planning in the acquisition lifecycle allows for informed design decisions and architectural trade space options that foster improved system efficiency and effectiveness in the face of the rapidly changing threats.

Several categories of trades occur throughout the acquisition lifecycle that may impact cybersecurity performance in DoD systems and networks. These include capability, performance, and cost trade-offs, and lesser trades made daily in engineering judgment as part of requirements development and design, as well as in configuration management throughout the lifecycle. The impacts of nonfunctional requirements (e.g., suitability, survivability, cybersecurity, interoperability, safety) are considered during functional performance trade-offs. All such categories of trades are discussed in the DoD 5000-series issuances.

For example, in support of the validation of the CDD (or equivalent requirements document), the PM may decide to conduct an SE trade-off analysis to show how cost varies as a function of system requirements (including KPPs), major design parameters, and schedule. The results would then be provided to the MDA to identify major affordability drivers and show how the program meets affordability constraints.

Additional trades may be considered between security controls, system functional performance requirements, and potential costs of an affordable set of mitigations that would reduce identified risks to an acceptable level. Risks identified through the TSN analyses will also inform these trades. Regardless of how and when the trades are discussed and completed, programs should:

- Modify the tailored set of controls based on the results of analyses and engineering trades.
- Ensure updates to tailored security controls set are reflected in the Security Plan.
- Ensure mitigations are documented and reflected in the updated PPP.
- Develop and map initial security specifications and requirements from the identified mitigations.
- Identify the strength of implementation and effectiveness of the updated tailored security control set.
- Review the residual risk and determine if additional security mitigations are warranted.

Figure 13 shows how SE and SSE, informed by TSN analyses and other program protection activities, affect the tailored set of controls implemented to protect the system based on updated cybersecurity and TSN risk assessments. The final set of tailored controls is documented in the Security Plan and approved by the authorizing official.

C.10 Systems Engineering Technical Reviews[37]

From a cybersecurity perspective, the PM, with support from the Lead Systems Engineer, should use the SETR process to integrate SE, program planning, and cybersecurity throughout the entire lifecycle of the system and demonstrate the system is able to meet its operational capability requirements and is trustworthy and resilient in the face of a capable cyber adversary. DoDI 5000.02 and DAG Chapters 4 and 13 describe the SETR process as a series of technical reviews and audits that are conducted at various points along the lifecycle of a program to evaluate progress for the system in development and maturity of the design, and serve as a basis for managing/reducing risk while transitioning between lifecycle phases. The reviews are intended to be event-driven and based on the entrance and exit criteria as documented in the SEP.

[37] See DAG Chapters 4 and 13 for more detail on the SSE and PPP aspects of the SETRs.

Annex D - Cybersecurity Test and Evaluation Considerations

D.1 Introduction

The overarching DoD cybersecurity acquisition policy is documented in DoDD 5000.01, *The Defense Acquisition System*, and DoDI 5000.02, *Operation of the Defense Acquisition System*. DoDD 5000.01 states, "Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.01E."

DoDI 5000.02 states, "Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01…should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, system engineering, and test and evaluation. Integration of the RMF in acquisition processes reduces required effort to achieve authorization to operate and subsequent management of security controls throughout the system life cycle."

Additionally, the Director, Operational Test and Evaluation has published specific procedures for the conduct of cybersecurity operational testing.[38] This guidance states in part that "the purpose of cybersecurity operational test and evaluation is to evaluate the ability of a unit equipped with a system to support assigned missions in the expected operational environment … Early involved of programs with the operational test community is required to ensure that system requirements are measureable and testable, and that the rationale behind the requirements and the intended operational environment are understood."

This annex will assist programs in integrating cybersecurity testing during both DT&E and OT&E. This testing, as well as all relevant SE, fraud prevention, validation, interoperability, and acquisitions processes, should be synchronized with the DoD RMF processes for assessment and authorization.

The PM is responsible for identifying the program's test team, including the Chief Developmental Tester and the lead T&E organizations, and for developing and implementing a robust cybersecurity T&E strategy. The goal of cybersecurity T&E is to improve the resilience of military capabilities before development is completed and production and deployment begin. Early discovery of system vulnerabilities can facilitate remediation to reduce the impact on cost, schedule, and performance. This annex provides an overview intended for the PM. DAG Chapter 9 provides detailed guidance for the Chief Developmental Tester and lead DT&E organizations. (https://acc.dau.mil/CommunityBrowser.aspx?id=504118)

[38] DOT&E Memorandum: "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" dated August 1, 2014

D.2 Cybersecurity Test and Evaluation

The focus of both developmental and operational cybersecurity T&E is to help programs and acquisition decision makers manage risks to operations in the cyberspace domain by identifying and resolving shortfalls as soon as possible. Figure 14 illustrates the procedures overlaid on a notional acquisition lifecycle.

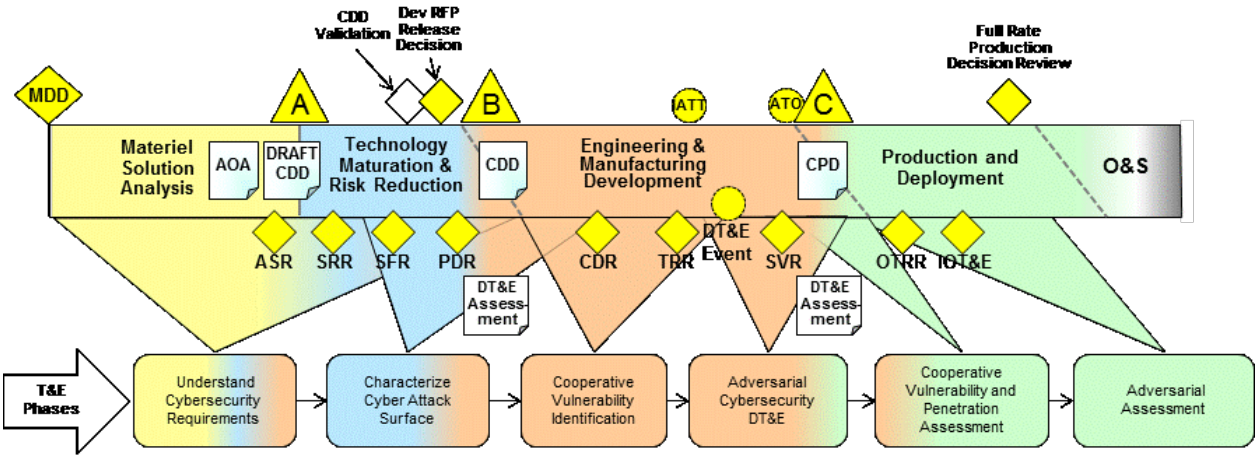


Figure 14 - Cybersecurity T&E Process Mapped to the Acquisition Lifecycle

Programs complete the full cybersecurity T&E process, regardless of the point at which they enter the acquisition cycle. If T&E in a realistic operational environment is not feasible because of operational risk, counterintelligence, or protection of penetration techniques, then alternative evaluation strategies will be identified (including use of dedicated cyber ranges) and included in an approved TEMP. The TEMP should define an integrated cybersecurity T&E strategy to assess the cybersecurity capability of the system. The integrated cybersecurity T&E strategy uses cybersecurity-related data from all available sources, including the RMF security assessments, security inspections, component/system/system-of-system tests, testing in an operational environment, and testing with systems and networks operated by representative end users and/or network service providers to ascertain the cybersecurity capability of a system. The T&E Evaluation Framework included in the TEMP must consider system cybersecurity requirements and correlate them with sources of information such as dedicated cybersecurity tests.

The following paragraphs describe the six phases of the cybersecurity T&E process. The PM is responsible for ensuring the process is adequately resourced and performed within the program.

D.2.1 Developmental Test and Evaluation

DT&E is performed as early as possible in the acquisition lifecycle to identify system vulnerabilities in order to facilitate remediation and reduce impact on cost, schedule and performance. For programs under DASD(DT&E) oversight, an evaluation of cybersecurity will be performed at Defense Acquisition Executive Summary reviews and in DT&E Assessments provided at major decision points, as required by DoDI 5000.02. The cybersecurity T&E phases supporting developmental test and evaluation are summarized below; detailed information of the implementation of these phases is included in the DAG, section 9.6.5.

D.2.1.1 Understand Cybersecurity Requirements

As early as possible within the acquisition process, the Chief Developmental Tester, in collaboration with the T&E Working-level Integrated Product Team (WIPT), examines the Acquisition Strategy, the capability requirements document, the Program Protection Plan, and all other documents and regulations to gain an understanding of the breadth and depth of the system's cybersecurity requirements (specified, implied, and essential). The Chief Developmental Tester and T&E WIPT will ensure system cybersecurity requirements are complete and testable. In addition, the T&E WIPT reviews threat documents to understand the cyber threats to the system. Based on the requirements review, the T&E WIPT constructs a T&E strategy to address the cybersecurity requirements and threat profiles. This phase will be performed iteratively, as system development proceeds.

D.2.1.2 Characterize the Cyber Attack Surface

The attack surface defines the system's exposure to reachable and exploitable vulnerabilities, to include any hardware, software, connection, data exchange, service, removable media, etc., that might expose the system to potential threat access. The T&E WIPT collaborates with engineering and system developers to determine and prioritize the elements and interfaces of the system that, based on criticality and vulnerability analysis, require specific attention in the cybersecurity section of the T&E strategy. The T&E WIPT updates the MS B (or relevant milestone) TEMP with plans for testing and evaluating the elements and interfaces of the system deemed susceptible to cyber threats.

D.2.1.3 Cooperative Vulnerability Identification

The Chief Developmental Tester defines vulnerability-type testing for contractor and government cybersecurity testing at the component and subsystem levels. This testing assists in refining the scope and objectives for subsequent cybersecurity T&E and is integrated to the greatest extent possible into the T&E program as a whole. Preparation for vulnerability testing is performed, in part, by understanding the cybersecurity kill chain (i.e., by considering how an adversary might exploit vulnerabilities). It is necessary to understand the sequence of adversary activities used to execute a cyber-attack. The vulnerabilities identified in this and previous phases should be resolved or mitigated before the program proceeds to a full end-to-end DT&E assessment.

D.2.1.4 Adversarial Cybersecurity DT&E

This phase is an end-to-end assessment in a representative mission context to evaluate the system's readiness for limited procurement/deployment and operational testing. This activity focuses on conducting a rigorous cybersecurity test in an environment as realistic as available and requires the use of a threat-representative test team that tests the potential and actual impacts to the system. Results of this testing will be included as part of the DT&E assessment, which typically occurs before MS C. Shortfalls identified in this and previous activities should be resolved before proceeding to OT&E, and program should plan sufficient time and resources for these resolutions.

D.2.2 Operational Test and Evaluation

Operational cybersecurity T&E is required to be conducted for all systems capable of sending or receiving digital information, including those that upload/download data by physical means or removable devices. The TEMP and Test Plan for cybersecurity OT&E should be structured in the two phases shown below with the goal of identifying all significant vulnerabilities and characterizing the operational risk imposed by them. Cybersecurity OT&E is informed by but not wholly satisfied by the RMF process. TEMPS and Test Plans for systems under OT&E oversight require DOT&E review and approval and must meet requirements defined in Attachments D and E of the DOT&E Memorandum "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs." [39]

D.2.2.1 Cooperative Vulnerability and Penetration Assessment

This phase will be conducted as an overt, cooperative, and comprehensive examination of the system to identify vulnerabilities and to characterize the system's operational cybersecurity status. This test event shall be conducted by a vulnerability assessment and penetration testing team through document reviews, physical inspection, personnel interviews, and the use of automated scanning, password tests, and applicable exploitation tools. The assessment must be conducted in the intended operational environment with representative operators to the greatest extent possible. This testing event may be integrated with DT&E activities, if conducted in a realistic operational environment and approved by the DOT&E. The minimum data required for this phase of testing is identified via Attachments A and B of the DOT&E Memorandum cited above.

D.2.2.2 Adversarial Assessment

This phase will assess the ability of a system to support its missions while withstanding validated and representative cyber threat activity. In addition to assessing the effect on mission execution, the test shall evaluate the ability of the system to detect threat activity, react to threat activity, and restore mission effectiveness degraded or lost due to threat activity. This test event must be conducted by an operational test agency employing a certified adversarial team to act as a cyber-aggressor. The adversarial assessment should include representative operators and users, local and remote cyber network defenders (including upper tier computer network defense providers), an operational network configuration, and a representative mission with expected network traffic[40]. Where necessary due to operational limits or security, tests may use simulations, closed environments, cyber ranges or other validated tools approved by DOT&E. The minimum data to be collected for this phase of testing is identified via Attachment C of the DOT&E Memorandum cited above, and is focused on determining the mission effects resulting from vulnerabilities or penetrations of the system under test.

D.3 Overarching Cybersecurity T&E Guidelines for the PM

The PM should ensure the following are implemented and appropriately resourced within the program:

---

[39] DOT&E Memorandum: "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" dated August 1st 2014.

[40] See section 9.6.5 of the DAG

- Test activities integrate RMF security controls assessments with tests of commonly exploited and emerging vulnerabilities early in the acquisition lifecycle.
- The TEMP details how testing will provide the information needed to assess cybersecurity and inform acquisition decisions. The TEMP must identify cybersecurity measures and resources and provide all information identified in the DOT&E Memorandum cited above.
- The cybersecurity T&E process requires the development and testing of mission-driven cybersecurity requirements, which may require specialized systems engineering and T&E expertise. The Chief Developmental Tester may request assistance from SMEs to implement the process. SMEs may be especially helpful in developing testable cybersecurity requirements that reflect:
  - Explicit risk management decisions related to potential harm arising through the acquired system
  - Realistic, achievable expectations for system cybersecurity capabilities
  - The system's role in a holistic cyber defense to achieve a resilient mission capability.
- The T&E WIPT seeks opportunities to improve efficiency by integrating cybersecurity into other planned T&E events.
- Sufficient time and test articles are made available for adversarial assessments in both developmental and operations test phases as these tests may interfere with other test objectives (such as availability or reliability tests).

Annex E - Cybersecurity Lifecycle and Sustainment Considerations

The purpose of the operations and support (O&S) phase (sustainment) is to execute the product support strategy, satisfy materiel readiness and operational support performance requirements, and sustain the system over its lifecycle (to include disposal). O&S is described in detail in the LCSP, initially developed during the Materiel Solution Analysis phase, and evolved during the TMRR and the EMD lifecycle phases when threat assessments, risk analyses, and early design decisions occur. Cybersecurity support needed in sustainment includes software support activities, help desk, vulnerability management, and assessing the risk of changes to the system, the evolving threat, and the operational environment.

It is recommended the Cybersecurity WIPT[41] or Logistics WIPT ensure required activities in the O&S phase are conducted in accordance with *DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)*, Step 6.

Cybersecurity activities in the O&S phase include:

Information Security Continuous Monitoring (ISCM): ISCM helps ensure the Cybersecurity Strategy is successfully implemented.[42] ISCM does not replace the requirement for system reaccreditation every three years; however, it is an enabler for continuous reauthorization. ISCM is also an enabler for the required annual RMF for DoD IT reporting requirements. Annual reviews are required by the Federal Information Security Management Act (FISMA) of 2002.

Information Assurance Vulnerability Alerts[43] (IAVAs): An IAVA is a notification of an operating system, utility, or application software vulnerability. IAVAs are distributed to all DoD computer installations and PMOs in the form of alerts, bulletins, and technical advisories identified by the US Cyber Command DoD Computer Emergency Readiness Team. Each IAVA is analyzed by a security engineer with applicable technical background and implemented if applicable, but only after regression testing to ensure the system continues to function. The acquisition PM should ensure all locations where the developed system is deployed receive, analyze, implement where applicable, and maintain an account of IAVAs. IAVAs can be tracked by the program or Component ISSO.

Warning Order (WARNORD)/Operation Order (OPORD): The WARNORD/OPORD replaces the Communications Tasking Order (CTO)/Fragmentary Orders (FRAGO)[44] outlining specific requirements for deployment and implementation of a capability on the Non-secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet).

---

[41] The Cybersecurity WIPT is sometimes organized as a cybersecurity sub-WIPT and is subordinate to the SE WIPT. A cybersecurity Support Working Group could also be subordinate to the Logistics (or Supportability or Sustainment) WIPT.

[42] Per DoDI 8510.01, Section f.(1).(a).1

[43] IAVAs are maintained on the DISA site. (http://iase.disa.mil)

[44] CTO/FRAGO requirements were originally published by the Joint Task Force Global Network Operations. The current WARNORDs and OPORDs are under the authority of US Cyber Command, which has supplanted the Joint Task Force Global Network Operations.

They are created to assist a system administrator or reviewer/auditor in assessing specified requirements. Each program logistics organization (either the PMO or appropriate logistics depot/organization) is responsible for analysis, implementation, and documentation of a specific WARNORD or OPORD. Analysis and compliance are mandatory. Note that WARNORDs/OPORDs are more than patches or configuration updates; they can be relatively extensive.

Software patches and updates: Many enterprises within the DoD automate patch updates and software updates for operating systems and DoD standard software applications.[45] For applications such as databases and developed applications, updates are scheduled. Software updates should be analyzed to determine if reauthorization is required. Patches usually address bug fixes and cybersecurity issues. Applying patches usually does not trigger reauthorization. Per DoDI 8500.01, Enclosure 3, paragraph 9.b.(11), "all IA products and IA-enabled products that require use of the product's IA capabilities will comply with the evaluation and validation requirements of Committee on National Security Systems Policy 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, June 2013, as amended."

National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation (https://www.niap-ccevs.org) is published on the NIAP-CCEVS Products Compliance List.[46] NIAP-certified products have been assessed from a security perspective, helping to reduce the existence of potential vulnerabilities. In most cases, the respective vendors continually maintain their products, mitigating vulnerabilities and distributing fixes to licensed users. Since these products have been evaluated, many of the system patches, security fixes, and version updates are pushed to systems connected to DoD networks. The CCEVS and the Unified Capabilities Requirements (UCR) are intended to complement each other in scope and capability, with minimal overlap.

Anti-virus/HIDS signatures are maintained and updated: Each DoD enclave ensures all hosts are configured with current anti-virus definitions and intrusion detection and prevention signatures. Updates should be pushed to each host weekly (or sooner in the case of a new known vulnerability). Most DoD installations facilitate this process using the HBSS.[47]

Firmware (e.g., Basic Input/Output System) is updated securely: Procedures and provisions for secure firmware updates may be defined as part of the system or component support manuals. Firmware updates are analyzed to determine if an increase in residual risk has occurred; if so, a reauthorization is required.

---

[45] Patches are supported for DoD-approved software applications. Signature updates are pushed using the Host-Based Security System (HBSS).

[46] Reference https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm.

[47] Since many bases/installations support HBSS and related activities, the PM's responsibility is minimal. It may be as simple as confirming anti-virus updates are furnished as part of an enterprise and documenting this fact in the Security Plan. For systems not connected to a network, the PM ensures a method for updating virus definitions is implemented. The PMO (through the ISSM or ISSO) documents the control is satisfied by the base/installation into the program's RMF database in the Enterprise Mission Assurance Support Service.

Equipment is updated securely: Procedures and provisions for secure hardware updates or replacement should be documented in system or component support manuals. Hardware updates are analyzed to determine if an increase in residual risk has occurred; if so, a reauthorization is required. During both the TMRR and EMD phases (as part of system and security requirements definition and solicitation of the development and production contract[s]), the PM should ensure that system and security requirements specifications mandate the use of DoD-approved products by the development and production contractor. Sources for approved hardware can be found on the DISA UC APL at https://iase.disa.mil. Where applicable, systems should operate within the DoDIN.

Reauthorization in accordance with DoD RMF requirements: Per DoDI 8510.01, Enclosure 6, para 2.f.(6).(a), "In accordance with Appendix III of OMB Circular A-130, systems must be reassessed and reauthorized every 3 years or as a result of a system update that negatively affects the security posture (whichever is less)." Program Offices or appropriate logistics organizations plan for this activity. The results of an annual cybersecurity review[48] or a negative change to the system or environment at any time (i.e., a change increasing the residual risk) may result in a need for reauthorization prior to the regular three-year reauthorization.

Local infrastructure: Site personnel maintain local site infrastructure, facility, physical, and procedural security requirements during sustainment.

The PMO itself may not execute[49] the activities during sustainment (i.e., some acquisition PMs are not responsible for system management throughout the entire O&S phase of the lifecycle). However, the PMO is active during all phases of the program acquisition lifecycle to ensure certain cybersecurity sustainment capabilities (e.g., continuous monitoring "agents") are incorporated into the system and the system is implemented such that cybersecurity protection is supported through the decommissioning/disposal phase.

During sustainment, due diligence should be maintained with regard to the cybersecurity posture. Should the threat change or a significant change to the system require a patch or system upgrade, then the PM should assess the fix by way of a vulnerability assessment (e.g., Blue Team activities) and/or penetration testing (e.g., Red Team activities) to ascertain the limitations and capabilities of the fix. The results of these assessments and tests help determine the effectiveness of implemented security controls that are monitored over time and updated or improved to address changes in threats, vulnerabilities, and the environment. Also any cybersecurity issues are identified, mitigated, and documented in the POA&M as the result of testing and audits.

Overview – Decommissioning/Disposal

The final phase of the acquisition lifecycle is the disposal and demilitarization of excess and surplus property. The DAG recommends surplus equipment be made available within the U.S. government to maximize the government's investment. One caveat is to ensure that

[48] Annual reviews are required by the Federal Information Security Management Act of 2002. These assessments are more along the lines of a checklist. Vulnerability assessments (e.g., Blue Team testing) and penetration tests (e.g., Red Team testing) are not included as part of the annual review.

[49] The PMO works with the cognizant local support organizations during earlier phases of development (TMRR and EMD) to define roles and responsibilities for sustainment. These are usually defined as part of the Logistics WIPT.

decommissioning and/or disposal of surplus equipment does not compromise classified or sensitive information. It is possible to minimize the need for abandonment or destruction, thus mitigating potential cybersecurity risks. During earlier phases (TMRR and EMD) and system design, the systems engineer supports the PM's plans for the system's demilitarization and disposal through the identification and documentation of hazards and hazardous materials related to the system, using MIL-STD-882E, DoD Standard Practice for System Safety.[50] From a cybersecurity perspective, the PM ensures a risk assessment is complete and any risks associated with surplus and disposal are mitigated. One of the more common risks is associated with data remanence. If not properly implemented, residual classified data and privacy data could be retained on media (e.g., disk drives, Universal Serial Bus drives) and memory that is no longer protected.

Sanitization can be achieved for nonvolatile media by simple overwrite or purging (e.g., multiple overwrites, or in cases of older media, degaussing). Volatile media can be sanitized by removal of power (e.g., Random Access Memory and some mobile device media). If no means of sanitization is possible or effective, destruction of the media is necessary. Per NIST SP 800-88, while some techniques may render it infeasible to retrieve the data through the device interface and to use the device for subsequent storage of data, the device is not considered destroyed unless data cannot be retrieved. Verification usually requires use of advanced laboratory techniques. For systems that process classified data, media destruction is required. Many media types are available, and there are different techniques and procedures for different types of media destruction. Per DoDI 8500.01, disposal and destruction of classified hard drives, electronic media, processing equipment components, and the like will be accomplished in accordance with CNSSI 4004.1.[51] Destruction can be achieved through disintegration, pulverizing, melting, and incineration. These methods are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Data remanence applies to any system and device with any kind of memory, disks, printers that contain memory, specialized devices, network routers, and associated equipment.[52]

The PM ensures challenges associated with destruction are addressed early in the acquisition lifecycle. Per DoDI 8510.01,[53] "once a system has been decommissioned, the Security Plan should be updated to reflect the system's decommissioned status and the system should be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in cybersecurity infrastructures that support the DoD Information Enterprise, such as key management, identity management, vulnerability management, and privilege management, should be reviewed for impact."

---

[50] DAG, para 4.3.18.7, Demilitarization and Disposal.

[51] *CNSSI No. 4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material*, August 2006.

[52] For specialized products such as controllers that contain volatile and non-volatile memory, vendors usually provide a function to clear memory. However, the clearing may not satisfy national and Service-specific clearing and purge requirements.

[53] DoDI 8510.01, Enclosure 6, paragraph 2.f.(7).

- For classified information, in addition to destruction, the system's status is documented and submitted to the responsible security officer.[54]
- If the media do not contain classified data, the PM should ensure a risk analysis is conducted early in the acquisition program lifecycle to ensure sensitive (e.g., Unclassified//For Official Use Only [U//FOUO], privacy data, and financial information) is rendered inaccessible.
- Systems that inherit security controls from a decommissioned system must re-evaluate their system and ensure the "dis-inherited" controls are implemented on their respective system. If a service level agreement (SLA) is in place, it no longer applies. Signatories of an SLA are notified of a system's decommissioning so they can satisfy their respective security controls.

[54] *NIST SP 800-88, Revision 1, Guidelines for Media Sanitization*, Table 5-1; Appendix A, Tables A-1 through A-9.

Annex F - Cybersecurity Risk Assessment Process

F.1 Cybersecurity Risk Assessments

Cybersecurity risk assessment is a key component of a holistic, organization-wide cybersecurity risk management process defined in NIST Special Publication 800-39. As depicted in Figure 15, the cybersecurity risk management process includes: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. This section focuses on assessing risk so the authorizing official may respond to risk appropriately. Risk monitoring activities inform the system's ATO and will prompt the authorizing official to respond accordingly.

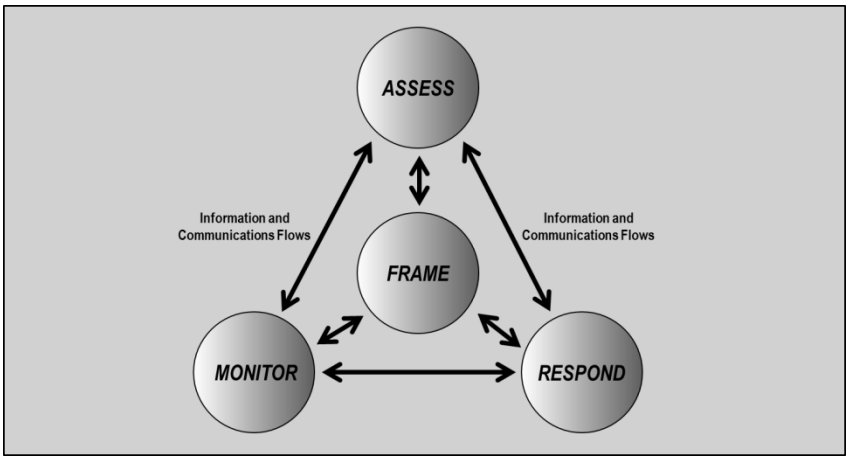


Figure 15. Risk Assessment within the Risk Management Process

Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) adverse impacts that would arise if the circumstance or event occurs and (ii) likelihood of occurrence. Cybersecurity risks are risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and PIT systems and reflect potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Note that the focus is on impact to the system's ability to support the mission, not impact to the IS/PIT system itself.

Cybersecurity risk assessment is the process of identifying, estimating, and prioritizing cybersecurity risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur. A risk model identifies risk factors. The risk factors of concern are threat sources, threat events, likelihood, vulnerabilities and predisposing conditions, and impact.

Figure 16 illustrates the risk model, including the risk factors discussed above and the relationship among them. The degree to which each risk factor is used in the risk assessment process depends on the availability and detail of information related to that risk factor. For example, detailed threat source or threat event data may not always be available, so risk assessors may need to make some assumptions. Any assumptions are clearly stated in the documentation of the risk assessment results (e.g., Security Plan, risk assessment report). Unlike assessing risk to acquisition program objectives, which the PM leads, these cybersecurity risk assessments can be led by the PM or the cybersecurity community throughout the lifecycle to inform tailoring of security controls and corresponding cybersecurity design requirements and

system updates based on mitigations to moderate and/or high risks. For example, when tailoring the controls, the PM tasks the ISSM and systems security engineers to perform the assessment and document the results in the Security Plan. The PM also uses cybersecurity and TSN risk assessments to make risk-based trade-offs that are explained/captured in acquisition and/or SE documentation. The SCA may examine these documents to understand design decisions. PMs support development of mitigation plans and incorporate approved materiel mitigation plans in their program cost, schedule, and performance plans.

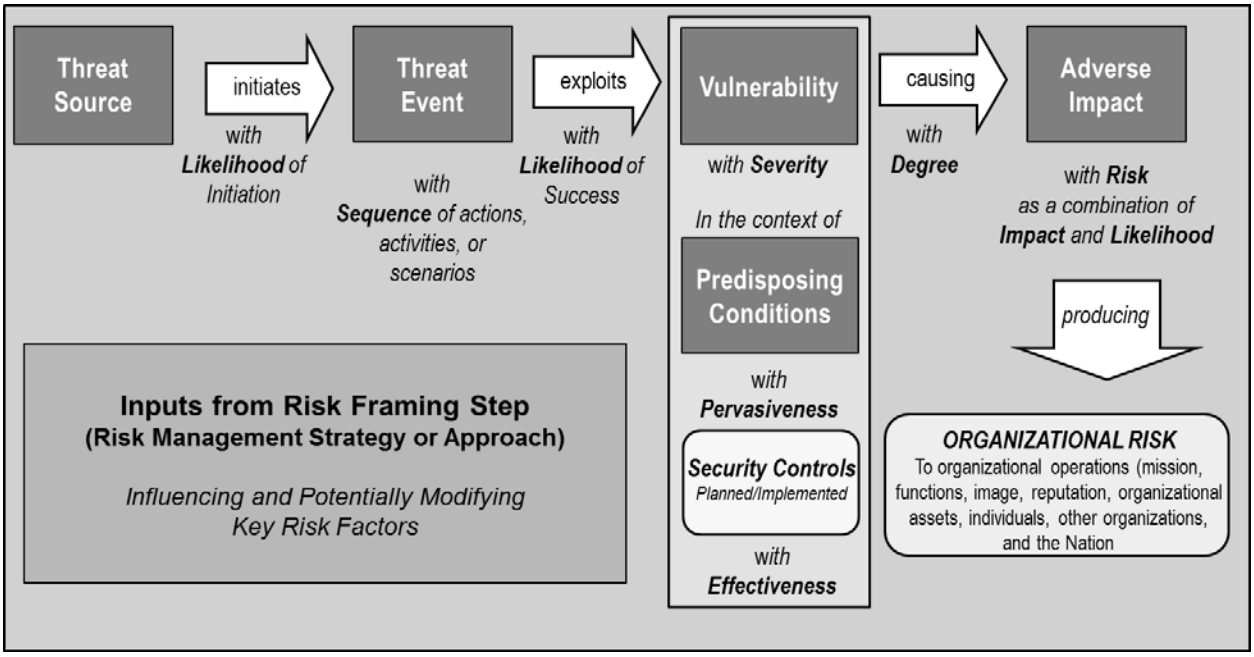


Figure 16. Generic Risk Model with Key Risk Factors

Risk assessments (formal or informal) are conducted at various steps in the acquisition lifecycle and at key steps in the RMF, including:

- Before each milestone and decision point.
- At each SETR (progressively more detailed as the concept evolves from conceptual architecture at ASR, to initial system-level design system performance requirements at SRR, to final system-level design the functional baseline at SFR, to preliminary item detail design at PDR, to detailed item final design at CDR).
- IS/PIT system categorization (to understand impact values for each information type processed by the system).
- Security control selection (to understand system-specific threats that may exploit vulnerabilities, thus driving the need to tailor security controls).
- Security control implementation (to identify, understand, and justify risk-based trade-offs).
- Security control assessment (to understand the severity of vulnerabilities created or not addressed by ineffectively implemented security controls, measured against likelihood and impact).

- IS/PIT system authorization (to ascertain, vet with stakeholders, and accept mission risk and/or community risk).
- Security control monitoring (to determine the impacts of proposed or imposed changes to the system, its environment, or its use).

The resulting risk rating is conveyed to the authorizing official, who responds in some manner (e.g., approve the Security Plan, authorize the system to operate, recommend or direct corrective actions to mitigate risk to an acceptable level) consistent with the organizational risk frame.

The DoD's cybersecurity risk assessment process is adopted from NIST SP 800-30. While the NIST process steps/tasks, lexicon, risk factors, definitions, and five-tier scale (see Figure 17) must be followed (to ensure reciprocity across the Federal, DoD, and Intelligence communities), the level of rigor is adjustable within each step/task. This flexibility is necessary because the information, expertise, and resources required to perform each step/task may not always be readily available. However, in communicating the results of any risk assessment, the level of rigor is explicitly identified per step/task.

The risk assessment process is composed of four steps: (i) prepare for the assessment; (ii) conduct the assessment; (iii) communicate assessment results; and (iv) maintain the assessment.

The appropriate risk model and analytic approach depend on where the system is in the acquisition lifecycle. If a risk model has been developed for a specific capability, that risk model should be used during the risk assessment process.

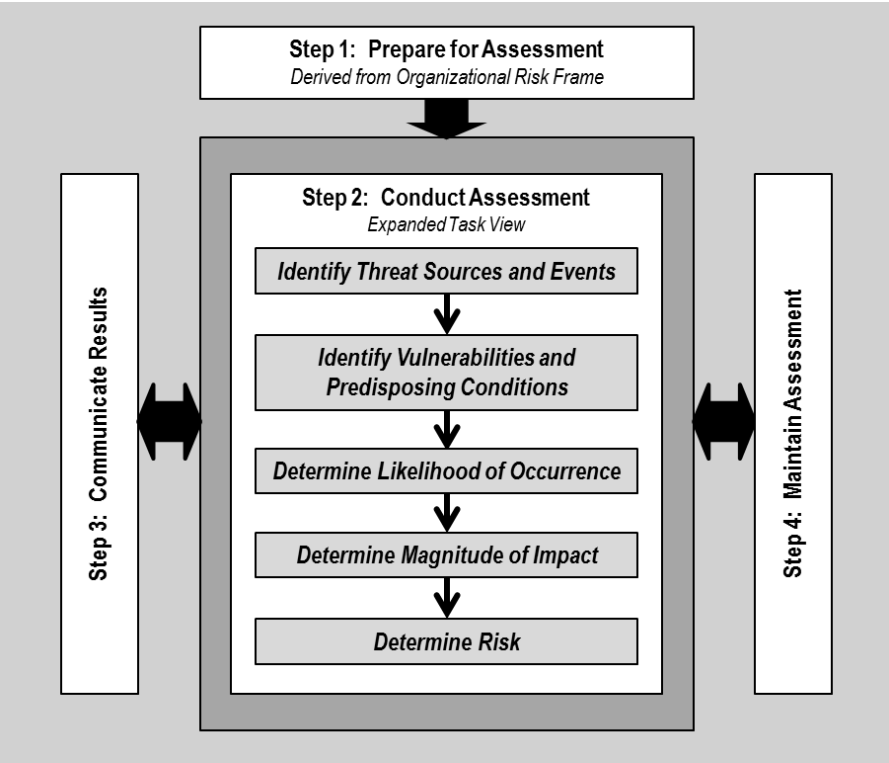


Figure 17. Risk Assessment Process

Risk is assessed quantitatively, qualitatively, or semi-qualitatively. Due to uncertainties and lack of quantifiable data, it is often necessary to use a semi-qualitative model or more often a qualitative model. Uncertainty is inherent in evaluation of risk, due to such considerations as: (i) limitations on the extent to which the future will resemble the past; (ii) imperfect or incomplete knowledge of the threat (e.g., characteristics of adversaries, including tactics, techniques, and

procedures); (iii) undiscovered vulnerabilities in technologies or products; and (iv) unrecognized dependencies, which can lead to unforeseen impacts.

Analysts use one of the following three approaches to arrive at a risk level: (i) threat oriented; (ii) asset/impact oriented; or (iii) vulnerability-oriented. NIST SP 800-30 primarily takes a threat-oriented approach, in which analysts begin with the possible threat events and determine the likelihood threat sources will initiate or cause those threat events to exploit vulnerabilities or predisposing conditions and cause an impact. The threat-oriented approach may be most appropriate during the system categorization and the selection of controls, as the technology is usually not selected at this point and the technical vulnerabilities cannot be known. An asset/impact-oriented approach starts with identification of impacts of concern to critical assets then identifies threat events that could lead to and/or threat sources that could seek those impacts. The asset/impact-oriented approach may be most appropriate when designing a system or to determine which components of a design need the most protection or should be re-designed to eliminate vulnerabilities or single points of failure. Following the security controls assessment, it is most appropriate to take a vulnerability-oriented approach, in which analysts begin with a set of predisposing conditions or weaknesses/deficiencies (e.g., non-compliant security controls) and estimate the likelihood threat sources will initiate or cause threat events that could exploit those vulnerabilities and cause an impact. Any of the approaches may be appropriate following authorization of the system, depending on whether a new threat or a new vulnerability is being assessed, or there is simply a need to determine the impact of proposed changes.

In determining the level of risk, consider that risk is a function of likelihood and the level of impact.[55] Likelihood is a function of the vulnerability or predisposing condition and the relevance of the threat. Vulnerability severity is a function of the raw vulnerability and the effectiveness of mitigation actions. The relevance of the threat is based on a non-adversarial threat source's range of effects or an adversarial threat source's capability, intent, and targeting. Table 5 is used to determine the risk based on the overall likelihood and the level of impact ratings. Similarly, a matrix could be used to determine the likelihood by placing the vulnerability/predisposing condition on the vertical axis and the threat relevance on the horizontal axis.

[55] NIST SP 800-30 defines impact level as "the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability." It defines the assigned impact value as "The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high."

Table 5. Level of Risk Combination of Likelihood and Impact[56]

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

As the risk model and analytical approach are considered for each risk assessment, an additional factor to be considered is alignment with existing or related risk management and risk assessment processes. In accordance with DoDI 5200.44, DoDI 5000.02, and DAG Chapter 13, TSN analysis is performed to protect mission-critical functions and components within covered systems. TSN analysis activities begin early in the lifecycle and are revised as a system design evolves and matures. The analysis is updated at each of the technical reviews to take into account the latest design and implementation decisions as well as additional threat and vulnerability information. For acquisition programs, this analysis is documented in the PPP. When applicable, cybersecurity risk assessment and TSN analysis activities and processes inform one another, to achieve a more cohesive and comprehensive cybersecurity risk picture for the system and program.

[56] NIST SP 800-30, Appendix I, Table I-2.

Annex G - Summary of Cybersecurity-Related Artifacts

A primary consideration for the PM relates to generation and use of cybersecurity-related artifacts. These artifacts provide essential information for both identifying achievable cybersecurity requirements and acquiring a system that meets these requirements. A goal of the new cybersecurity approach is to maximize use of existing acquisition program management, systems engineering, test and evaluation, configuration management, and risk management documentation and artifacts. As such, the Program Office and assessment community should work together to identify and document where the related cybersecurity information can be found in existing documentation as opposed to creating new cybersecurity artifacts. Major artifacts appear in alphabetical order by name in Table 6. See DoDI 8510.01 and the RMF Knowledge Service for further information on individual cybersecurity RMF artifacts. In some cases, more than one approval authority is listed, separated by a semicolon. In these instances, the first authority listed applies to programs under Office of the Secretary of Defense (OSD) oversight, and the second applies to those under Component-level oversight.

Table 6. Cybersecurity-Related Artifacts

	Lifecycle Event										
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other	Source	Approval Authority	Responsible Role
RMF Authorization Decision Document						•	•	•	DoDI 8510.01	AO	AO
	The authorization decision document includes the authorization decision, terms and conditions for the authorization, authorization termination date, and risk executive (function) input (if provided) and is an output of the Security Authorization Package.										
Initial Capabilities Document (ICD)		•							DoDI 5000.02 CJCSI3170.01 JCIDS Manual	JROC; Component	UR, PM, SE
	ICDs and their associated operational context and threat summaries provide information to help define the cybersecurity requirements that are needed to ensure that the overall capability fulfills the identified capability gap.										
Capability Development Document (CDD)			•	•					DoDI 5000.02 CJCSI3170.01 JCIDS Manual	JROC; Component	UR, PM, SE
	A draft CDD is completed for MSA and approved for the Development RFP Release Decision Point. The CDD contains KPPs, mission requirements, and cybersecurity requirements that mature in a mission-relevant state throughout the EMD phase. A Requirements Definition Package or equivalent DoD Component-validated document will satisfy this requirement for certain information systems.										

	Lifecycle Event										
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other	Source	Approval Authority	Responsible Role
Capability Production Document (CPD)						•			DoDI 5000.02 CJCSI 3170.01 JCIDS Manual	JROC; Component	UR, PM, SE
	The CPD reflects the operational requirements, informed by EMD results, and details the performance expected of the production system.										
Capstone Threat Assessment	•							•	DIAI 5000.002	DoD IC	DoD IC
	Capstone Threat Assessments (CTAs) address, by warfare area, current and future foreign developments which challenge U.S. warfighting capabilities. Updated every two years, CTAs present the validated DoD Intelligence Community position with respect to those warfare areas and maintain projections of technology and adversary capability trends over the next 20 years. CTAs will constitute the primary source of threat intelligence for the preparation of DIA or Service-validated threat assessments (e.g., STARs) and threat portions of documents supporting the JCIDS process. The Cyberspace Operations CTA addresses adversary threat capabilities within the cyberspace domain and is available at (SIPR) http://www.intelink.sgov.gov/wiki/Capstone_Threat_Assessment.										
Cost Analysis Requirements Description (CARD)			•	•	•	•	•	•	DoDI 5000.02	PEO	PM
	The CARD formally describes the acquisition program for purposes of preparing the Program Office lifecycle cost estimate, DoD Component Cost Estimate, and the independent cost estimate (as applicable). A CARD is prepared by the Program Office and approved by the DoD Component Program Executive Officer.										
Cybersecurity Strategy (formerly Information Assurance Strategy [IAS])			•	•	•	•	•		DoDD 8500.01 DoDI 5000.02 DoDI 8580.1	DoD CIO; Component CIO	PM
	The Cybersecurity Strategy is an iterative document that reflects both the program's long-term approach for, as well as its implementation of, cybersecurity throughout the program lifecycle. The Cybersecurity Strategy should be used as a tool for PMs, AOs, cybersecurity, and acquisition oversight authorities to plan for, document, assess, mitigate, and manage risks as the program matures. The PM updates and maintains the Cybersecurity Strategy and ensures it matures with the system design throughout the system lifecycle.										

	Lifecycle Event								Source	Approval Authority	Responsible Role
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other			
DT&E Assessment					•	•			DoDI 5000.02	DASD (DT&E); Component T&E	DASD (DT&E)
	For programs subject to OSD oversight, DASD(DT&E) prepares a DT&E assessment that includes cybersecurity for the MDA to review and for use during the MS C decision. Programs not subject to OSD oversight follow the Component policy. The DT&E assessment is an in-depth analysis beginning at MS B that assesses the results of DT&E (to include all cybersecurity T&E) and the progress against key performance parameters, key system attributes, and critical technical parameters in the TEMP. This analysis should include cybersecurity. Inclusion of the Security Assessment Report results within the DT&E assessment is recommended. For details on the DT&E assessment, refer to the DAG, Chapter 9, T&E.										
Information Support Plan (ISP)				•		•		•	DoDI 5000.02 DoDI 8330.01 DoDD 8320.02	PEO	CE
	Format, content, and process for the ISP provide a mechanism to identify and resolve implementation issues related to IT and National Security System (NSS) infrastructure and support elements. ISPs identify IT and NSS information needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency.										
Life-Cycle Sustainment Plan (LCSP)			•	•	•	•	•	•	DoDI 5000.02 IAW 5000.02 Table 2	MDA	PM
	The LCSP is prepared by the PM and approved by the MDA and is the basis for activities conducted during the O&S phase.										
[RMF] Plan of Action and Milestones (POA&M)					•	•	•	•	DoDI 8510.01	CIO	PM
	The system level POA&M addresses: (1) why the system needs to operate; (2) any operational restrictions imposed to lessen the risk during a conditional authorization; (3) specific corrective actions necessary to demonstrate that all assigned security controls have been implemented correctly and are effective; (4) the agreed-upon timeline for completing and validating corrective actions; and (5) the resources necessary and available to properly complete the corrective actions. POA&Ms may be active or inactive throughout a system's lifecycle as deficiencies are newly identified or closed.										

	Lifecycle Event								Source	Approval Authority	Responsible Role
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other			
Program Protection Plan (PPP)			•	•	•	•	•		DoDI 5000.02 DoDI 5200.39	MDA	CE
	Program protection is the integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle. The process of preparing a PPP is intended to help Program Offices consciously think through which technology, components, and information need to be protected and to develop a plan to provide that protection. Once a PPP is in place, it should guide Program Office security measures and be updated as threats and vulnerabilities change or are better understood. The PPP should be a usable reference within the program for understanding and managing the full spectrum of program and systems security activities throughout the acquisition lifecycle. The PPP contains the information someone working on the program needs to carry out his or her program protection responsibilities, and it should be generated as part of the program planning process.										
Request for Proposal (RFP)			•	•		•	•		DoDI 5000.02 FAR Subpart 15.203	PM, MDA	PM
	Includes specifications and Statement of Work.										
[RMF] Security Authorization Package						•	•	•	DoDI 8510.01	Authorizing Official	PM, SCA
	The security authorization package consists of artifacts developed through RMF activities and informs the development of an authorization decision document. The package contains the Security Plan, SAR, POA&M, and any supporting evidence and analysis. The package must also contain, or provide links to, the appropriate documentation for any security controls that are being satisfied through inheritance (e.g., security authorization packages, contract documents, MOAs, and SLAs).										

	Lifecycle Event								Source	Approval Authority	Responsible Role
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other			
[RMF] Security Assessment Plan				•	•	•			DoDI 8510.01	Authorizing Official or AODR	SCA
	The Security Assessment Plan provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. The SCA develops the Security Assessment Plan, and the authorizing official reviews and approves the plan. The SCA ensures that the coordination of activities is documented in the Security Assessment Plan and the program test and evaluation documentation, including the TEMP, to maximize effectiveness, reuse, and efficiency.										
[RMF] Security Assessment Report (SAR)					•	•	•	•	DoDI 8510.01	SCA	SCA
	The SAR contains the assessment plan, controls to be assessed, and assessment results, as well as any artifacts produced during the assessment (e.g., output from automated test tools or screen shots that depict aspects of system configuration). The SCA ensures coordination with Chief Developmental Tester for inclusion within the DT&E Assessment in support of MS C.										
[RMF] Security Plan			•	•	•	•	•	•	DoDI 8510.01	Authorizing Official or AODR	ISSM
	The Security Plan provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements, and includes implementation status, responsible entities, resources, and estimated completion dates. The plan can also contain, as supporting appendixes or as references, other key security-related documents that may aid in understanding the implementation of security requirements, such as a risk assessment results, trade-off analyses, privacy impact assessments, system interconnection agreements, contingency plans, security configurations, configuration management plans, and incident response plans. The ISSM, with assistance from the PM, requirements sponsor, user representative, and SSE, develops the Security Plan that is approved by the authorizing official.										

	Lifecycle Event								Source	Approval Authority	Responsible Role
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other			
System Threat Assessment Report (STAR)			•	•		•	•		DoDI 5000.02 DIAD 5000.200 DIAI 5000.002	Per DoDI 5000.02	DoD IC
	The STAR provides a holistic assessment of enemy capabilities to neutralize or degrade a specific U.S. system by addressing both threat-to-platform and threat-to-mission. The STAR is intended to serve as the authoritative threat document supporting the acquisition decision process and the system development process.										
System Engineering Plan (SEP)			•	•	•	•			DoDI 5000.01	DASD(SE); Component SE	PM, CE
	The SEP captures the program's current status and evolving SE implementation and its relationship to the overall program management effort. The plan documents key technical risks, processes, resources, metrics, SE products, and completed and scheduled SE activities, along with other program management and control efforts such as the Integrated Master Plan (IMP), Risk Management Plan (RMP), Technical Performance Measures, and other documentation fundamental to successful program execution. The SEP should be consistent with and complementary to the Acquisition Program Baseline, Acquisition Strategy, TEMP, PPP, LCSP, and other program plans as appropriate. In addition, the SEP should define the roles, responsibilities, and membership of the SE, program protection, T&E, and WIPTs required to comprehensively address cybersecurity. In support of execution of the SEP, the program should ensure the schedules and cost estimates accurately reflect the SE elements of cybersecurity activities, and these activities also flow into the work breakdown structure supporting the TMRR RFP. (Reference: DAG, Chapter 4, Systems Engineering)										
Threat Analysis Center (TAC) Assessment								•		DIA	DIA
	The threat assessment provided by DIA SCRM TAC utilizes intelligence and counterintelligence to assess risks that may be introduced intentionally or unintentionally by a particular supplier. TAC Assessments are used in conjunction with the TSN analysis, and folded into the PPP. Although the PPP is required to be updated more often, there may not be a TAC update at every milestone. TAC input should be coordinated as necessary.										

	Lifecycle Event								Source	Approval Authority	Responsible Role
	Pre MDD	MDD	MS A	Dev RFP Rel	MS B	MS C	FRP/ FD	Other			
Test & Evaluation Master Plan (TEMP)			•	•	•	•	•		DoDI 5000.02	DASD(DT &E); Component T&E	PM, Chief Dev Tester
	The TEMP serves as the overarching document for managing a T&E program. PMs develop a draft TEMP in support of the Development RFP Release Decision Point decision to be used during the EMD phase. The TEMP includes sufficient detail to support development of other test-related documents. PMs structure a T&E program strategy with inclusion of cybersecurity to provide knowledge to reduce risk in acquisition and operational decisions. The evaluations of all available and relevant data and information from contractor and government sources develop that knowledge. The evaluation should focus on providing essential information to decision makers, specifically with regard to attainment of technical performance attributes and an assessment of the system's missions operational effectiveness, operational suitability, and survivability or operational security. The evaluation framework supports estimates for test resource requirements and provides a basis for determining test program adequacy and assessing risk margins within the T&E plans and events. For details and content of the TEMP, refer to the DAG, Chapter 9, T&E.										

Annex H - Cybersecurity Request for Proposal Considerations

NOTE: This sample RFP language is a reference only and is not intended to be used as-is. The sample language can assist the PM and his/her team in developing an RFP that reflects the specific stakeholder cybersecurity requirements and the specifics of the solution under development. It is important for the PM and his/her team to integrate cybersecurity into their SSE approach to achieve the most cost-effective system security.

H.1 Overview

To achieve a cost-effective cybersecurity implementation, the program manager (PM) and the functional staff must recognize systems security engineering begins at or before the material solution analysis (MSA) phase. Cybersecurity considerations, incorporated into the larger SSE activities, are grounded in a technical approach with understandable, achievable, testable, and measurable performance requirements.

The PM must understand the cybersecurity requirements prior to release of any solicitation, starting with the Technology Maturation and Risk Reduction RFP and Draft CDD at MS A. Subsequent RFPs must address user-validated cybersecurity requirements in the CDD and CPD (or equivalent capability requirements documents). To do this, the PM ensures all cybersecurity capabilities (provided via Draft CDD, CDD, or CPD) are decomposed into the government-owned technical requirements baseline and included within the RFP to the contractor(s), enabling the contractor to properly respond to the RFP and giving the PM an early understanding of the cybersecurity impact to the program. Many cybersecurity capability requirements are included within the mandatory system survivability key performance parameter (KPP). However, PMs should review all KPPs and KSAs to ensure they have a full understanding of the breadth and depth of cybersecurity requirements. The PM, in reviewing the draft CDD, will provide feedback to the user representative in regards to technical and affordability feasibility. This should be done by a Systems Security Engineer or a similarly qualified individual on the PM's staff.

Often, these derived cybersecurity requirements span across the government acquisition organization (the PMO), the government user, and the system definition and development contractor. The PM accounts for and tracks all cybersecurity requirements, not just those put on contract to the development contractor. All cybersecurity requirements should be part of the government-owned requirements baseline and verification cross reference matrix/index, allowing the validation approach for each requirement to be integrated early into the SSE and T&E activities.

Key cybersecurity considerations when beginning solicitation activities are as follows:

- Ensure program planning documentation, even in draft, reflects achieving stakeholder and program cybersecurity requirements.
- Ensure an integrated cybersecurity strategy and approach addresses the total lifecycle of the system.
- Ensure the specific cybersecurity test ranges/facilities and test support equipment are identified for each type of testing.
- Ensure cybersecurity requirements are part of the budget and cost estimates, as part of the program's plans and schedule.
- Consider cybersecurity aspects of Joint Interoperability Test Command interoperability and Net-Ready KPP certification.

H.2 Request for Proposal (RFP) Language

Sample RFP language is available from each DoD Component and applies to RFPs and contracts intended to procure all information technology, including Platform IT (PIT) systems. The items below are aligned with the structure of a typical solicitation, providing cybersecurity considerations for each portion of the solicitation. The PM reviews and adjusts the language used for solicitations to ensure alignment with the overall SSE goals and objectives and the acquisition type.

A – Solicitation/contract form. No cybersecurity-specific information is anticipated in this section.

B – Supplies or services and prices/costs. Review all CDRL deliverables for inclusion of cybersecurity execution support (e.g., data rights, test data, test plans, source code deliveries, prototype quantity, and delivery times/location).

C – Description/Specifications/Statement of Work.

- Clearly define, and state in performance-based terms directly tied to program objectives, all cybersecurity requirements levied on the contractor.
- Include cybersecurity system/technical requirements in the system/technical requirements document (SRD/TRD). If requiring the contracted developer to define the formal technical requirements in a system/item performance specification, add that technical requirements definition work task to the SOW/SOO and reference a system/item performance specification data deliverable in an associated CDRL. Provide the list of applicable security controls (after initial tailoring), with the understanding that they will be further tailored during system development.
- Identify the categorization of the system, including overlays. This includes listing the applicable controls that will inform the developer's security requirements and design the contractor is required to implement and assess, to meet requirements.
- Ensure all CDRLs adequately address cybersecurity execution support (e.g., data rights, test data, test plans, source code deliveries, prototype quantity, and delivery times and location).

- Identify any specific design, contractor testing, or contractor artifacts that enable meeting the cybersecurity requirements based on system categorization, applicable RMF controls, and which controls the contractor will be authorized to assess.

D – Packaging and marking. No cybersecurity-specific information is anticipated in this section.

E – Inspection and acceptance. Ensure the acquisition team has developed a tailored quality assurance surveillance plan to monitor contractor performance. This may include cybersecurity considerations.

F – Deliveries or performance. Ensure cybersecurity-related items are addressed as any other type of requirement would be, for example:

  - Identify the required number (sample size) of test articles.
  - Establish a delivery location for test articles along with schedule.
  - Identify contractor-acquired property.
  - Identify PM's desire to have contractor support personnel available to repair or provide reachback for the contractor's product during cybersecurity effort.
  - Identify contractor property needed as spares during the testing.

G – Contract administration data. No cybersecurity-specific information is anticipated in this section.

H – Special contract requirements. List applicable cybersecurity special contract requirements (e.g., handling of data, software license management, and maintenance).

  - If there is a desire to use contractor facilities for cybersecurity initial testing, state that need in the solicitation and resulting contract.

I – Contract clauses. Cybersecurity-specific contract clauses should be considered (e.g., the DFARS clause: Safeguarding Unclassified Controlled Technical Information).

J – List of Attachments. Applicable cybersecurity attachments should be considered (e.g., a DoD Component RMF Guide).

K – Representations, Certifications, and Other Statements of Offerors or Respondents. Include requests for certifications that support the cybersecurity strategy (e.g., NSA certifications of cryptographic algorithms or equipment, and certification of cross domain solutions).

L – Instructions, Conditions, and Notices to Offerors or Respondents.

- Describe the contractor management structure for cybersecurity (e.g., the experience of cybersecurity staff, predicted staffing levels, and the application of cybersecurity best practices and its alignment with the contractor management structure for SSE and T&E).

- Define the contractor's responsibilities for cybersecurity and the alignment of those responsibilities in contrast to the government for required SSE and T&E activities (e.g., contractor cybersecurity testing, developmental testing, and integrated testing).
- Describe the contractor's approach for technical data, including management, ownership, control, timely access, and delivery of all cybersecurity data, including raw test data, to support the evolving technical baseline.
- Define CDRLs and select applicable DIDs. Identify any cybersecurity-related data products contractors must provide. Determine the applicability of DIDs in support of cybersecurity efforts.
- Determine applicability of commercial certifications of materiel or products.
- Describe the contractor's approach for use of commercial and/or government Blue and/or Red Teams during cybersecurity testing.
- Describe the contractor's access to government cyber ranges (e.g., DoD Enterprise Cyber Range Environment (DECRE)) during cybersecurity testing.

M – Evaluation Factors for Award.

- Prior performance in integrating cybersecurity considerations into the program's SE, SSE, and T&E processes.
- Meet cybersecurity workforce certification and training requirements in DoDD 8570.01 and DoD 8570.01-M, and investigative requirements per DoDI 8500.01.
- Prior performance in supporting the government to achieve cost-effective cybersecurity authorizations to operate.
- Define measures and metrics clearly to evaluate qualification of contractor cybersecurity staff.
- Define clear minimum thresholds for performance objectives for cybersecurity.
- Convey critical program objectives in the evaluation criteria.

H.3 Additional Request for Proposal Information

For additional information:

- On January 23, 2014, the USD (AT&L) signed the *Final Report of the Department of Defense and General Services Administration Improving Cybersecurity and Resilience through Acquisition*. The report provides a path forward for better aligning Federal cybersecurity needs, risk management, and acquisition processes. See the report for recommendations related to RFPs. (http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf)
- On November 19, 2013, the DoD issued an amendment to the DFARS "which will require defense contractors to incorporate established information security standards on their unclassified networks, and to report cyber-intrusion incidents that result in the loss of unclassified controlled technical information from these networks." (http://www.regulations.gov/#!documentDetail;D=DARS_FRDOC_0001-0658)

- DoD Systems Engineering Initiatives for Program Protection and System Security Engineering website – Online resource for program protection and SSE information with links to related policy, guidance, acquisition regulations, papers and presentations, and collaboration with industry. (http://www.acq.osd.mil/se/initiatives/init_pp-sse.html)
- The following contractual language is provided by NSA for procurements involving commercial technologies to help ensure commercial component vendors meet CNSS Policy No. 11 requirements: "*Technologies for [Program X] shall be procured in accordance with CNSSP No. 11, "National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products." In addition, technologies shall be procured which have been validated by Common Criteria Testing Labs, in accordance with the National Information Assurance Partnership (NIAP) Protection Profiles (PPs). Where a PP exists but the desired product has not been validated against it, [Program X] shall direct the desired vendor to have their product validated against the appropriate, corresponding PP. For National Security Systems (NSS) where classified data is being protected at rest or in transit by commercial products, technologies from the Commercial Solutions for Classified (CSfC) Components List shall be used, in accordance with NSA's published CSfC Capability Packages. Capability Packages and the CSfC Components List can be found by visiting the CSfC Components List page (https://www.nsa.gov/ia/programs/csfc_program/component_list.shtml). NIAP-validated products can be found at the NIAP website on the CCEVS Product Compliant List (https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm) page.*"

For additional reference:

- CDRLs, defense and federal specifications and standards. (https://assist.dla.mil/online/start/)
- Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance and Information. (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html)
- Federal Acquisition Regulation Part 15.203, Request for Proposal. (https://acquisition.gov/far/current/html/Subpart%2015_2.html#wp1125252)
- Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Dec 2006. (http://www.acq.osd.mil/se/docs/Integrating-SE-Acquisition-Contracts_guide_121106.pdf)
- Incorporating Test and Evaluation into DoD Acquisition Contracts, Oct 2011. (https://acc.dau.mil/rfpbuddy)

Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals, January 2014 (http://www.acq.osd.mil/se/docs/SSE-Language-for-TSN-in-DoD-RFPs.pdf)

Annex I - Cybersecurity Glossary of Terms and Acronyms

This section defines acronyms and key terms used in the document.

Table 7. Terms

Term	Definition	Source
Authorization to Operate **(ATO)**	The official management decision issued by an AO to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Per DoDI 8500.01, for full and independent operational testing, an ATO (rather than an IATT) may be required if operational testing and evaluation is being conducted in the operational environment or on deployed capabilities. In this case, the ATO should be reviewed following operational testing and evaluation for modification as necessary in consideration of the operational test results	CNSSI 4009
Blue Team	The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers, (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks: 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).	CNSSI 4009
Cyber Attack Surface	The collection of vectors threat sources may use to access, disrupt, destroy, or deny use of a network service, information system, or other forms of a computer-based system. Vectors include, but are not limited to: hardware flaws, firmware, communications links, physical interfaces, software, open communication ports, and	

Term	Definition	Source
	communication protocols.	
Cyber Resilience or Operational Resilience	Cyber resilience is the resilience of DoD systems to cyber attacks. *Cyber* is broadly used to address the components and systems that provide all digital information, including weapons/battle management systems, IT systems, hardware, processors, and software operating systems and applications, both stand-alone and embedded. *Resilience* is defined as the ability to provide acceptable operations despite disruption: natural or man-made, inadvertent or deliberate. *Operational resilience* is the ability of systems 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.	DoD Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, January 2013, Cyber Resilience; DoDI 8500.01, Operational Resilience
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	DoDI 8500.01
IATT	Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization. Per DoDI 8510.01, IATTs should be granted only when an operational environment or live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical), and should expire at the completion of testing (normally for a period of less than 90 days). Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for	CNSSI 4009

Term	Definition	Source
	operational purposes during the IATT period). The application of an IATT in support of DT&E needs to be planned, resourced, and documented within the program T&E plan.	
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency directly or is used by a contractor under a contract with the executive agency which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.	CNSSI 4009
Mission-Critical Function	Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed, and is identified through a Criticality Analysis.	DoDI 5200.44
Platform Information Technology (PIT)	IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems.	DoDI 8500.01
PIT System	A collection of PIT within an identified boundary under the control of a single authority and security policy. The system may be structured by physical proximity or by function, independent of location. Owners of special-purpose systems (i.e., platforms), in consultation with an authorizing official, may determine that a collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms	DoDI 8500.01

Term	Definition	Source
	they support. PIT systems are designated as such by the responsible OSD or DoD Component Heads or their delegates and authorized by an authorizing official specifically appointed to authorize PIT systems.	
Program Manager	The individual with responsibility responsible and accountability for the implementation of DoD security requirements in accordance with DoDI 8500.01. Program Managers, under the supervision of Program Executive Officer (PEOs) and Component Acquisition Executives (CAEs), are expected to design acquisition programs, prepare programs for decisions, and execute approved program plans. <u>Information Assurance</u>. Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.01E, reference (k). Note: DoDI 8500.01, March 14, 2014, replaced DoDD 8500.01E and DoDI 8500.02.	DoDI 8500.01 DoDI 5000.02 DoDD 5000.01
Red Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. For additional information on their application during T&E, refer to Defense Acquisition Guidebook, Chapter 9, T&E	CNSSI 4009

Term	Definition	Source
Risk (cyber)	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (a) the adverse impacts that would arise if the circumstance or event occurs; and (b) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.	CNSSI 4009
Software Assurance	The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.	DoDI 5200.44
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	CNSSI 4009

Term	Definition	Source
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. This should be planned for and resourced within the programs T&E Master Plan and executed within DT&E (during the EMD phase), utilizing a Blue Team type activity to assist in the assessment (refer to Defense Acquisition Guidebook, Chapter 9, T&E).	NIST SP 800-39

Table 8. Acronyms

ACAT	Acquisition Category
AO	Authorizing Official
AoA	Analysis of Alternatives
AODR	Authorizing Official's Designated Representative
APB	Acquisition Program Baseline
APCL	Approved Products Compliance List
APL	Approved Products List
AS	Acquisition Strategy
ASR	Alternative Systems Review
ATC	Approval to Connect
AT&L	Acquisition, Technology and Logistics

ATO	Authorization To Operate
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CA	Criticality Analysis
CAN	Control Area Network
CARD	Cost Analysis Requirements Description
CBT	Computer-Based Training
CCEVS	Common Criteria Evaluation and Validation Scheme
CCI	Control Correlation Identifier
CCTL	Common Criteria Testing Laboratory
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDS	Cross Domain Solution
CE	Chief Engineer
CGS	Community Gold Standard
C-I-A	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer

CJCSI	Chairman of the Joint Chief of Staff Instruction
CL	Confidentiality Level
CM	Countermeasure
CMVP	Cryptographic Module Validation Program
CNDSP	Computer Network Defense Service Provider
CNSSI	Committee on National Security Systems Instruction
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COTS	Commercial off-the-Shelf
CPI	Critical Program Information
CPD	Capability Production Document
CRC	Cyclic Redundancy Check
CTA	Capstone Threat Assessment
CTO	Communications Tasking Order
DAA	Designated Accrediting Authority (older term replaced with Authoring Official)
DAES	Defense Acquisition Executive Summary
DAG	Defense Acquisition Guidebook

DASD	Deputy Assistant Secretary of Defense
DAU	Defense Acquisition University
DBS	Defense Business System
DEMIL	Demilitarization
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	DoD IT Portfolio Repository
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoDIN	DoD Information Networks
DOORS	Dynamic Object Oriented Requirements System
DOT&E	Director of Operational Test & Evaluation
DR	Deficiency Report
DSAWG	Defense Information Assurance Security Accreditation Working Group

DSPAV	DoD-specific assignment values
DT&E	Developmental Test and Evaluation
eMASS	Enterprise Mission Assurance Support Service
EMD	Engineering & Manufacturing Development
FCB	Functional Capability Board
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
FRAGO	Fragmentary Orders
FRP	Full Rate Production
FRP/FD	Full Rate Production / Full Deployment
GAO	Government Accountability Office
GOTS	Government off-the-shelf
HBSS	Host-Based Security System
HIDS	Host Intrusion Detection System
IA	Information Assurance
IAS	Information Assurance Strategy (older term, now called Cybersecurity Strategy)
IASE	Information Assurance Support Environment

IATT	Interim Authorization To Test
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
ICD	Initial Capabilities Document
ICS	Industrial Control Systems
ILA	Independent Logistics Assessment
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IO	Information Owner
IOT&E	Initial Operational Test and Evaluation
IPT	Integrated Product Team
IS	Information System
ISCM	Information Security Continuous Monitoring
ISP	Information Support Plan
ISRMC	Information Security Risk Management Committee
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISR	In-Service Review

IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council
KPP	Key Performance Parameter
KS	Knowledge Service
KSA	Key System Attribute
LCSP	Life-Cycle Sustainment Plan
LFT&E	Live Fire Test and Evaluation
MAC	Mission Assurance Category
MAIS	Major Automated Information System
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision
MO	Mission Owner
MOSA	Modular Open Systems Approach
MS	Milestone
MSA	Materiel Solution Analysis
NIAP	National Information Assurance Partnership
NIPRNet	Non-secure Internet Protocol Router Network

NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
NSS	National Security System
NTOC	National Threat Operations Center
NVD	National Vulnerability Database
O&S	Operations and Support
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OIPT	Overarching Integrated Product Team
OPORD	Operation Order
OSA	Open Systems Architecture
OSD	Office of the Secretary of Defense
OTA	Operational Test Agency
OT&E	Operational T&E
P&D	Production and Deployment
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PEO	Program Executive Office

PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
PPP	Program Protection Plan
RA	Risk Assessment
RAR	Risk Assessment Report
RASCI	Responsible, Accountable, Supportive, Consulted, Informed (one form of a Responsibility Assignment Matrix)
RFP	Request for Proposal
RMF	Risk Management Framework
RMP	Risk Management Plan
RTM	Requirements Traceability Matrix
SAR	Security Assessment Report
SCA	Security Control Assessor (RMF terminology)
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
SDD	System Design Document

SDS	System Design Specification
SE	Systems Engineering
SEP	Systems Engineering Plan
SETR	Systems Engineering Technical Review
SFR	System Functional Review
SIPRNet	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SME	Subject Matter Expert
SP	Special Publication
SPS	System Performance Specification
SRD	System Requirements Document
SRG	Security Requirements Guide
SRR	System Requirements Review
SSE	Systems Security Engineering
STAR	System Threat Assessment Report
STIG	Security Technical Implementation Guide
TA	Threat Assessment
TAC	Threat Analysis Center

T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
TSN	Trusted Systems and Networks
TTP	Tactics, Techniques, and Procedures
UABS	Unmanned Aerial Bomber System
UC	Unified Capabilities
UCDSMO	Unified Cross Domain Services Management Office
UCR	Unified Capabilities Requirements
USD	Under Secretary of Defense
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
VA	Vulnerability Assessment
VM	Vulnerability Management
WARNORD	Warning Order
WIPT	Working-level Integrated Product Team

Annex J - Training

A variety of training resources are available to support the program manager (PM) and the PM's team in understanding and integrating cybersecurity, the risk management framework (RMF), and related topics. PMs need to ensure that personnel with cybersecurity responsibilities implementing RMF are properly trained in their job roles. This annex provides some key information about the training resources available.

J.1 DoD Risk Management Framework (RMF) Training

J.1.1 DISA Training

The Defense Information Systems Agency (DISA) is responsible for the Department of Defense (DoD)-wide RMF training program and has developed two high-level introductory training modules[57]. The purpose and goal of these two training modules are to inform learners about organizational and individual responsibilities in regard to DoDI 8500.01 and DoDI 8510.01. The primary target audience is all DoD personnel involved in DoD cybersecurity and DoD IT risk management. Instructionally, the training modules assume that the audience may have limited knowledge of the subject matter.

The modules introduce concepts of cybersecurity and overarching guidance on how to manage risks to information and information systems under the DoD RMF in order to operate approved systems. They also provide the guidance and references necessary to support a successful cybersecurity program under the new RMF policies.

The DISA training modules are posted on the Information Assurance Support Environment (IASE) portal at http://iase.disa.mil/rmf/rmf-training.html. The RMF training modules have also been taped by an instructor and will be posted once they are approved by the public affairs office and the closed captioning is finalized. The instructor-led Defense Connect Online course will be approximately three to four hours in length.

While not required, it is recommended that PMs attend the high-level RMF training to gain an understanding of the RMF process as it applies to DoD IT and PIT.

Another RMF high-level introductory training opportunity is available at https://acc.dau.mil/CommunityBrowser.aspx?id=693410&lang=en-US or

https://dap.dau.mil/daustream/Pages/AssetList.aspx?Asset-id=2070318.

This recorded briefing by the Chief of Cybersecurity Joint Information Environment Integration & Compliance, Deputy Chief Information Officer for Cybersecurity, Cybersecurity Implementation & Integration Directorate discusses:

- Why DoD is transitioning from the traditional DIACAP to a new six-step RMF for IT
- RMF overview and applicability within DoD

[57] Additional courses are planned.

- Alignment of DoD with the risk management approach of other Federal Agencies
- Timelines for implementation

The 90-minute briefing was originally given on 15 January 2014 at a Defense Acquisition University (DAU) Hot Topic Forum. The associated slides are also posted on the above DAU site.

DISA is also currently developing a new authorizing official RMF training course (two to three hours) that will replace the old DAA DIACAP course. This computer-based training (CBT) course should be available in the fall of 2014.

DISA's IASE is a "one-stop-shop" for education, training, and awareness in information assurance and cybersecurity. The site offers training materials and hosts an online classroom offering courses. The IASE can be accessed at http://iase.disa.mil/index2.html.

J.1.2 Defense Acquisition University (DAU) Continuous Learning Modules

CLE 074 – Cybersecurity throughout DoD Acquisition

This is the primary module for PMs to learn about cybersecurity and RMF. This five-hour module provides the foundational knowledge PMs and other acquisition professionals need. This information includes basic cybersecurity concepts, why it is important to integrate cybersecurity into the acquisition process, and the process used to integrate key cybersecurity activities into acquisition.

CLE 012 – DoD Open Systems Architecture

Designed for PMs, this two-hour module introduces DoD open systems architecture (OSA), explains OSA principles from a business and a technical perspective, and provides examples of successfully implemented OSA programs, as well as sources that can assist an organization in implementing OSA.

CLE 022 – Program Managers Introduction to Anti-Tamper

This three-hour module introduces the PM to the steps involved in integrating anti-tamper into a program or project to protect DoD critical program information (CPI). The student will learn the importance of anti-tamper, the threats to critical DoD technology, current DoD initiatives and programs designed to mitigate threats, how to plan for effective use of anti-tamper, and how anti-tamper can be effectively integrated into the overall program.

J.1.3 DAU Courses

DAU online course – IRM 101 – Basic Information Systems Acquisition

Within the framework of a program office IPT, this 30-hour online course covers introductory-level concepts in DoD information systems and software acquisition management. Key areas covered include DoD regulatory and technical frameworks, common software risks, software and system architectures, information assurance, lifecycle reviews, and software development and integration processes.

IRM 202 – Intermediate Information Systems Acquisition

This two-week classroom course focuses on the application of DoD policies, concepts, and best practices for the management and acquisition of software-intensive and IT systems. Exercises, lectures, group discussion, and labs are used to cover topics ranging from strategic planning, cybersecurity, architectures, advancing technologies, requirements management, cost estimation, metrics, process maturity, quality, and testing, among other areas.

J.2 Other DoD Training Resources

Further information and training material for PMs and their support staff will be available via the DAG, Chapter 7 (https://acc.dau.mil/CommunityBrowser.aspx?id=511590), DAU Continuous Learning Module (https://acc.dau.mil/CommunityBrowser.aspx?id=18914), and DoD SE guidance (http://www.acq.osd.mil/se). Transition information for cybersecurity professionals is available on the RMF Knowledge Service (https://rmfks.osd.mil/).

The DoD Systems Engineering/Systems Analysis office has developed training materials that will be incorporated into courses offered by the DAU, as well as some continuing education courses periodically offered through private industry and professional organizations. Check the DoD Systems Engineering website (http://www.acq.osd.mil/se/) for the latest information, contacts, and news about upcoming events.

J.3 Non-DoD Cybersecurity Training Open to DoD Personnel

NIST offers a two-hour CBT course titled Applying the Risk Management Framework to Federal Information Systems (http://csrc.nist.gov/groups/SMA/fisma/rmf-training.html). Even though this is a NIST-developed course, it is beneficial to DoD personnel since DoD RMF policies are heavily dependent upon NIST guidance.

The purpose of this course is to provide individuals new to risk management with an overview of a methodology for managing organizational risk—the RMF. This course describes at a high level the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step.

Annex K - References and Resources

K.1 References

DoD Policies and Guidance

- **DoDD 5000.01 – The Defense Acquisition System**
  - Outlines the DoD system for managing investments in technologies, programs, and services necessary to achieve the National Security Strategy and support the United States Armed Forces.
  - http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf
- **DoDI 5000.02 – Operation of the Defense Acquisition System**
  - Establishes management framework for translating approved capability needs and technology opportunities into stable, affordable, and well-managed acquisition programs for weapon systems, services, and information systems.
  - http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf
- **Defense Acquisition Guidebook** (https://dag.dau.mil/)
  - **Chapter 4, "Systems Engineering"**
    - Establishes the technical framework for delivering material capabilities to the warfighters.
    - https://acc.dau.mil/dag4
  - **Chapter 7, "Acquiring Information Technology"**
    - Describes policies for the acquisition of IT, including NSS;
    - Section 7.5 explains requirements for IA and provides links to resources for developing an IA strategy.
    - https://acc.dau.mil/dag7
  - **Chapter 9, "Test and Evaluation"**
    - Describes processes and procedures for planning and executing an effective and affordable T&E program in the DoD acquisition model.
    - https://acc.dau.mil/dag9
  - **Chapter 13, "Program Protection"**
    - Establishes regulatory requirements for Program Protection Plans at Milestones A, B, C, and FRP/FDD.
    - Provides implementation guidance for TSN analysis and CPI protection; describes SSE activities throughout the Defense acquisition lifecycle.
    - https://acc.dau.mil/dag13
- **DoDI 5205.13 – Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities**
  - Establishes policies for protecting unclassified DoD information transiting or residing on unclassified DIB information systems and networks, in view of cyber threats.

- http://www.dtic.mil/whs/directives/corres/pdf/520513p.pdf

- **DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD**
  - Outlines requirements and assigns responsibilities for Counterintelligence, Security, and System Engineering support for identification and protection of CPI.
  - http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

- **DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)**
  - Establishes policies for minimizing risk that warfighting capabilities will be impaired due to vulnerabilities in system design or subversion of mission-critical functions or components.
  - http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf

- **DoDI 8330.01 – Interoperability of Information Technology (IT), Including National Security Systems (NSS)**
  - Establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of IT and NSS.
  - http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf
- **DoDI 8500.01 – Cybersecurity**
  - Establishes the DoD cybersecurity program to protect and defend DoD information and IT.
  - Replaces DoDD 8500.01, Information Assurance (IA), and DoDI 8500.02, Information Assurance (IA) Implementation.
  - http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
- **DoDI 8510.01 – Risk Management Framework (RMF) for DoD Information Technology (IT)**
  - Establishes policies for implementing RMF for DoD IT and policies for managing lifecycle cybersecurity risks to DoD IT.
  - Replaces DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP).
  - http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
- **DoDI 8582.01 – Security of Unclassified DoD Information on Non-DoD Information Systems**
  - Establishes policy for managing the security of unclassified DoD information on non-DoD information systems.
  - http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf
- **Information Assurance Support Environment (IASE)**
  - Online cybersecurity reference website; includes links to STIGs and CCIs

- http://iase.disa.mil/

- **JCIDS Manual – Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)**
  - Outlines procedures for operation of the JCIDS, and interactions with other departmental processes to facilitate the development of capability solutions for warfighters.
  - https://dap.dau.mil/policy/Documents/2012/JCIDS%20Manual%2019%20Jan%202012.pdf

- **DoD Risk Management Guide for Acquisition Systems**
  - Assists PMs, program offices, and their IPTs in effectively managing risks within their acquisition programs. This guide contains baseline information and explanations for a well-structured high-level risk management program.
  - https://acc.dau.mil/rm-guidebook

- **PPP Outline and Guidance Memo, July 2011**
  - Provides outline and tables with example content to assist with PPP development.
  - http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf

- **Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals, January 2014**
  - Intended for use by DoD PMs preparing RFPs for major defense acquisitions.
  - http://www.acq.osd.mil/se/docs/SSE-Language-for-TSN-in-DoD-RFPs.pdf

Committee on National Security Systems Publications

https://www.cnss.gov/CNSS/issuances/Issuances.cfm

- **CNSSP No. 22 – Policy on Information Assurance Risk Management for National Security Systems**
  - Establishes the requirement for enterprise IA risk management within the national security community, and provides a framework for decision makers to evaluate, prioritize, and mitigate IA risks.
  - http://niatec.info/GetFile.aspx?pid=590

- **CNSSI No. 1253 – Security Categorization and Control Selection for National Security Systems**
  - Establishes processes for categorizing NSS and the information they process, and outlines procedures for selecting security controls.
  - http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf

- **CNSSI No. 4009 – National Information Assurance (IA) Glossary**
  - Reconciles the differences between the definitions of terms used by the DoD, Intelligence Community (IC), and civil agencies and promotes consistency in the usage of related and dependent terms.
  - https://www.cnss.gov/CNSS/issuances/Instructions.cfm

National Institute of Standards and Technology Publications

http://csrc.nist.gov/publications/

- **NIST SP 800-30, Rev 1 – Guide for Conducting Risk Assessments**
  - Provides procedures and guidance for conducting information security risk assessments for federal information systems.
  - http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- **NIST SP 800-37, Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach**
  - Provides guidance on applying RMF to federal information systems, to include security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
  - http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- **NIST SP 800-39 – Managing Information Security Risk – Organization, Mission, and Information System View**
  - Provides guidance for managing information security risk to organizational missions, operations, assets, and individuals resulting from the use of federal information systems.
  - http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- **NIST SP 800-53, Rev. 4 – Security and Privacy Controls for Federal Information Systems and Organizations**
  - Provides a catalog of security and privacy controls for federal information systems and organizations, and processes for selecting controls to protect organizational missions, operations, assets, and individuals from various threats, including cyber attacks, natural disasters, structural failures, and human errors.
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- **NIST SP 800-53A, Rev. 1 – Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans**
  - Provides guidelines for constructing effective Security Assessment Plans, and provides procedures to enable the assessment of security controls used in federal information systems.
  - http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
- **NIST SP 800-82, Rev. 2 – Guide to Industrial Control Systems (ICS) Security**
  - Provides guidance on how to secure industrial control systems, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as programmable logic controllers, while addressing their unique performance, reliability, and safety requirements.
  - http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_draft.pdf

- **NIST SP 800-160 – Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (INITIAL PUBLIC DRAFT)**
  - Provides engineering-driven activities required to develop a more defensible and survivable IT infrastructure—including the component products, systems, and services that compose the infrastructure. The document infuses SSE techniques, methods, and practices into those systems and software engineering processes to address security issues from a perspective of stakeholder requirements and protection needs, and to use established organizational processes to ensure that such requirements and needs are addressed early in and throughout the lifecycle of the system.
  - http://csrc.nist.gov/publications/PubsSPs.html
- **NIST SP 800-60, Rev 1 - Guide for Mapping Types of Information and Information Systems to Security Categories**
  - Provides assistance to Federal government agencies to categorize information and information systems. The document's objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.
  - http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
  - http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
- **NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**
  - Specifically addresses assessment and analysis of security control effectiveness and of organizational security status in accordance with organizational risk tolerance. Security control effectiveness is measured by correctness of implementation and by how adequately the implemented controls meet organizational needs in accordance with current risk tolerance (i.e., is the control implemented in accordance with the security plan to address threats and is the security plan adequate). Organizational security status is determined using metrics established by the organization to best convey the security posture of an organization's information and information systems, along with organizational resilience given known threat information.
  - http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

K.2 Additional Resources

- **Community Gold Standard (CGS) for Information Assurance (IA) –**
  - The CGS is led by the Information Assurance Directorate at the NSA and provides comprehensive IA guidance for securing enterprises.
  - https://www.iad.gov/iad/CGS/cgs.cfm
- **Cyber Security & Information Systems Information Analysis Center (CSIAC)**

- The CSIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC). The CSIAC, one of three IACs sponsored by DTIC, performs the Basic Center of Operations (BCO) functions necessary to fulfill the mission and objectives applicable to the DoD Research, Development, Test and Evaluation (RDT&E) and Acquisition communities' needs. These activities focus on the collection, analysis, synthesizing/processing and dissemination of Scientific and Technical Information (STI).
- https://www.csiac.org

- **Defense Acquisition University website**
  - Online presence for DAU, offering everything from formal courses and continuous learning modules to knowledge sharing assets and consulting tools, all of which are intended to help students develop and manage acquisition programs, projects, and systems.
  - https://dap.dau.mil/
- **Defense Acquisition Portal**
  - DAU-maintained website providing acquisition information for all DoD Components and across all functional acquisition disciplines. Serves as the central point of access for all AT&L resources and information, and communications about acquisition reform.
  - https://dap.dau.mil/Pages/Default.aspx/
- **Defense Acquisition University (DAU) Glossary of Defense Acquisition Acronyms and Terms**
  - https://dap.dau.mil/glossary/Pages/Default.aspx/
- **DoD Cybersecurity Policy Chart**
  - The goal of the DoD Cybersecurity Policy Chart is to capture applicable policies in a helpful organizational scheme. The format is designed to provide additional assistance to cybersecurity professionals navigating their way through policy issues.
  - http://iac.dtic.mil/csiac/download/ia_policychart.pdf
- **Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) website**
  - Online presence for the DoD SE Directorate includes links to information about SE, SSE, and program protection, as well as other SE policy and guidance documents, education and training materials, and additional acquisition program management resources. Check the website for the latest directorate information, contacts, and news about upcoming community outreach activities.
  - http://www.acq.osd.mil/se/
- **DoD Systems Engineering Initiatives for Program Protection and Systems Security Engineering website**

- Online resource for program protection and SSE information and links to related policy, guidance, acquisition regulations, papers and presentations, and collaboration with industry.
- http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

- **Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE)**
  - DISA's "one stop shop" for information and guidance about IA. Includes information, references, training materials, and links to supporting elements activities on a wide range of IA, cybersecurity, and related topics.
  - http://iase.disa.mil/

- **DoD Risk Management Framework (RMF) Knowledge Service (KS)**
  - Official DoD site for enterprise RMF policy and implementation guidelines. This site provides cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in RMF.
  - https://diacap.iaportal.navy.mil/ks/Pages/default.aspx/

- **National Information Assurance Partnership (NIAP) and COTS Product Evaluations website**
  - The NSA manages the NIAP, a federal program to help consumers and producers of IT meet the security testing needs. Through the NIAP's CCEVS, approved Common Criteria Testing Laboratories (CCTLs) evaluate commercial off-the-shelf (COTS) products. The CCEVS Validation Body provides technical guidance to CCTLs, validates the results of IT security evaluations for conformance to the International Common Criteria for IT Security Evaluation, and serves as an interface to other nations for the recognition of such evaluations.
  - http://www.nsa.gov/ia/business_research/partnerships_with_industry/niap_and_cots_product_evaluations.shtml/

- **National Vulnerability Database (NVD)**
  - The NVD is the federal government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol. This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.
  - http://nvd.nist.gov/

- **Unified Cross Domain Services Management Office (UCDSMO)**
  - Provides centralized coordination and oversight of all cross domain initiatives across the DoD and the IC. UCDSMO developed the CDS Overlay (CNSSI No. 1253, Appendix F, Attachment 3) to ensure that solutions implementing cross domain capabilities protect the information and networks that they connect with from compromise and disclosure. UCDSMO developed a Cross Domain Risk Model to

categorize the threats and the risks to NSS information and networks when implementing a CDS.

- NIPRNet Site: https://intelshare.intelink.gov/sites/ucdsmo/
- SIPRNet Site: http://intelshare.intelink.sgov.gov/sites/ucdsmo/
- JWICS Site: http://intelshare.intelink.ic.gov/sites/ucdsmo

K.3 Other Reports, Publications and Products

Acquisition of Information Technology

- **DOT&E Guidance Memorandum Procedures for OT&E of Cybersecurity in Acquisition Programs**
  - http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf
- **Defense Science Board Task Force report on DoD Policies and Procedures for the Acquisition of Information Technology,** March 2009
  - http://www.acq.osd.mil/dsb/reports/ADA498375.pdf
- **Improving Cybersecurity and Resilience through Acquisition - Final Report of the Department of Defense and General Services Administration,** January 2014
  - http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf
- **National Defense Industrial Association (NDIA) System Assurance Committee – Engineering for System Assurance,** October, 2008
  - http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf
- **Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations,** December 2012
  - http://www.acq.osd.mil/ie/energy/library/ICS%20Handbook%20Dec%2019.pdf

Resiliency

- **"Cyber Mission Resilience: Mission Assurance in the Cyber Ecosystem,"** Cross Talk Magazine, September/October 2012
  - http://www.crosstalkonline.org/storage/issue-archives/2012/201209/201209-Peake.pdf
- **Defense Science Board Task Force report on Resilient Military Systems and the Advanced Cyber Threat**, January 2013
  - http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

- **"Evaluating the Impact of Cyber Attacks on Missions,"** by Scott Musman, Aaron Temin, Mike Tanner, Dick Fox, and Brian Pridemore, The MITRE Corporation, 2010
  - http://www.mitre.org/sites/default/files/pdf/09_4577.pdf
- "**Achieving Mission Resilience for Space Systems,"** Aerospace Report Crosslink Magazine, Spring 2012
  - http://www.aerospace.org/2013/07/29/achieving-mission-resilience-for-space-systems/

Annex L - Other Cybersecurity Considerations

Annex L includes five key sections:

1. Risk Management Framework (RMF) Background Information
2. Cross Domain Solutions (CDS) Information
3. Questions PMs Can Ask to Determine if Cybersecurity is Integrated into Defense Acquisition Programs
4. Information Systems and IT Products
5. Platform IT (PIT) and PIT systems

L.1 Risk Management Framework Background Information

In 2006, the Chief Information Officers (CIO) of the Office of the Director of National Intelligence (ODNI) and Department of Defense (DoD), as well as others, created a Certification and Accreditation transformation activity to address problems with the government's approach to cybersecurity. The following problems were identified:

- A compliance mindset was employed with regard to cybersecurity.
- There was a heavy emphasis on paperwork, generally required every three years.
- Different agencies and departments used different cybersecurity controls and processes.
- Agencies did not accept each other's certification results, resulting in lack of reciprocity and wasted resources from redoing assessments that had already been done.
- Some of the PIT examples were the responsibility of other program managers outside the purview of the acquisition community.

DoD is moving to a risk-based approach to address these problems. Often, PMs did not understand what they were required to do to implement effective cybersecurity. All of these challenges needed to be addressed in a manner in which the DoD, intelligence community (IC), and civil sector (represented by the National Institute of Standards and Technology (NIST)) could all agree.

To address these problems, DoD and ODNI leadership agreed upon seven transformation goals:

1. Define a common set of impact levels; adopt and apply those levels across the federal government.
2. Adopt reciprocity as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.
3. Define, document, and adopt common security controls.
4. Adopt a common security lexicon—providing a common language and common understanding of terms.
5. Institute a senior risk executive function, which bases decisions on an "enterprise" view of risk considering all factors, including mission, IT, budget, and security.
6. Incorporate information security into Enterprise Architectures and deliver security as a common enterprise service across the federal government.

7. Enable a common process that incorporates information security within the lifecycle processes and eliminates security-specific processes.

Three years later in 2009, DoD, ODNI, the Committee on National Security Systems, and NIST established the Joint Transformational Task Force[58] and agreed to joint development of five core documents, all of which have been published, although they continue to be revised and updated.

- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012
- NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.

The replacement of the DoDI 8500.2 IA controls with the NIST SP 800-53 security controls is a direct result of the transformation effort, especially transformation goal #3. This facilitates moving the government from supporting multiple, disparate cybersecurity guidelines and standards to a single unified framework. The adoption of the RMF process can be traced back to transformation goal #7. The premise that the RMF activity should be risk based can be traced back to transformation goal # 5.

The replacement of the DIACAP with the RMF is a significant milestone in moving the government and DoD toward meeting some of the cybersecurity transformation goals. Other goals could take several more years to be fully implemented.

This document explains the changes DoD is implementing to integrate cybersecurity into the program acquisition lifecycle. PMs are asked to do the following:

- Build cybersecurity capabilities into the design, development, acquisition, operations, and sustainment of defense capabilities and systems.
- Assess their programs for potential cybersecurity threats, vulnerabilities, and weaknesses within a structured risk management framework.
- Address cyber-related needs and concerns earlier in acquisition lifecycles before design trades are made.

---

[58] The Government Accountability Office (GAO) has been positively impressed by this work (GAO publication 10-916, *Progress Made on Harmonizing Policies and Guidelines for National Security and Non-National Security Systems*), noting that "This harmonized security guidance is expected to result in less duplication of effort and more effective implementation of controls across multiple interconnected systems."

L.2 Cross Domain Solutions (CDS) Information

A CDS is a form of controlled interface that provides the ability to access or transfer information manually or automatically between different security domains. While a CDS provides the ability to share information across security domains, it also provides a level of protection for the information and enclaves to which it connects.

A CDS is implemented as part of an information system or PIT system and is authorized under the full RMF process. As stated in DoDI 8510.01, enclosure 6, authorizing officials must take into consideration the security impact of the CDS operation when making an authorization decision. The requirements for confidentiality and/or integrity of information being transferred across security domains, and the ability of the CDS to meet those requirements, are critical to the decision-making process.

Implementing a CDS introduces additional cybersecurity considerations and risks to the connected enclaves and therefore requires additional scrutiny during assessment and authorization processes. Authoritative guidance for CDS is provided in the following:

- DoD Chief Information Officer and Intelligence Community Chief Information Officer Memorandum, "Use of Unified Cross Domain Management Office (UCDMO) Baseline Cross Domain Solutions (CDSs)," December 1, 2011
- Chairman of the Joint Chiefs of Staff Instruction 6211.02D, "Defense Information Systems Network (DISN) Responsibilities," January 24, 2012.

In response to the authorities outlined in the above documents, the UCDSMO developed guidance to ensure that solutions implementing CDS protect the information and networks to which they connect from compromise and disclosure. During the MSA phase of the acquisition lifecycle, all systems that provide CDS should utilize the CDS Overlay (CNSSI No. 1253, Appendix F, Attachment 3) when performing their control selection and tailoring. This will ensure that the requirements critical to the implementation of a CDS are addressed.

The UCDSMO developed a Cross Domain Risk Model to categorize the threats and the risks to NSS information and networks when implementing a CDS. The Cross Domain Risk Model should be used when performing risk assessments of CDS throughout the entire acquisition lifecycle and assessment and authorization processes.

Beyond the T&E performed by the program throughout the acquisition lifecycle, Chairman of the Joint Chief of Staff Instruction (CJCSI) 6211.02D, enclosure C, allocates responsibility for performing CDS certification testing to DIA and NSA in accordance with UCDSMO guidance and applicable DoD and IC assessment and authorization requirements. The UCDSMO guidance for performing the certification testing is defined in the CDS Security Assessment Process Guide. In addition, the UCDSMO's Security Assessor's Guide provides specific guidance on how to test the security controls in terms of CDS. Both documents should be utilized when a security assessment is performed on a CDS as part of the assessment and authorization processes.

L.3 Questions Program Managers Can Ask to Determine if Cybersecurity is Integrated into Defense Acquisition Programs

- Is cybersecurity integrated into solution architectures and is it aligned with enterprise/segment/reference architectures? (Chief Engineer/Lead Systems Engineer/SSE)

- Early in the lifecycle during requirements and architecture definition and design, has the developer and/or Chief Engineer/Lead Systems Engineer/SSE tried to model or assess the mission impact of cyber incidents (i.e., estimating mission impact by comparing model measures of effectiveness with and without the effects of different/evolving cyber attacks)? Dynamic mission modeling allows for timing and duration information to differentiate between attacks than can be recovered from quickly and attacks that take much longer. This modeling will enable design and development of more attack-resistant systems that can operate through cyber attacks and can also support operations with better, more targeted responses to attacks. One example of the mission impact assessment is described in an article in *Modeling & Simulation Journal*, "Evaluating the Impact of Cyber Attacks on Missions," Summer 2013, pages 25–35. The article refers to a large body of existing work, tools, and techniques that address mission modeling. (Developer and/or Chief Engineer/Lead Systems Engineer/SSE)

- Did you appoint an ISSM (IA Manager under DIACAP) in writing? The ISSM is responsible for establishing, implementing, and maintaining the cybersecurity program for the system being acquired. The ISSM is also responsible for documenting the RMF authorization process (formerly DIACAP), and chairing the Cybersecurity WIPT. (PM)

- Did you establish a Cybersecurity WIPT during the MSA phase? The project members on the Cybersecurity WIPT should have the systems expertise necessary to support the development of the cybersecurity strategy (formerly the acquisition IA strategy). The Cybersecurity WIPT should be chaired by the ISSM or designee and should consist of SMEs familiar with the system being acquired, the intended use of the system, and the operational and system architectures within which the system will function. As the operational and system views of the architectures mature, the WIPT should conduct consultations into the principal systems with which the system being acquired will interface. Consider Cybersecurity WIPT membership from: the user community (e.g., user representative, requirements/resource sponsor, Joint Staff); authorizing official staff (e.g., authorizing official designated representative) (formerly DAA); SCA staff (formerly CA); OSD Cybersecurity RMF points of contact in DoD CIO, DASD(SE) (if they have oversight), and DASD(DT&E) (if they have oversight), System Threat Assessment Report representative, enterprise/segment/reference and solution architecture representatives; and representatives from engineering/SE (including program protection/SSE representative), acquisition, and the Chief Developmental Tester. (PM)

- Does the Cybersecurity Strategy describe:
    - The overarching technical approach to secure the system by applying the RMF throughout the acquisition lifecycle (and its subsequent implementation)

- How the program's cybersecurity requirements are traced through the security controls and into the acquisition baselines and system design
- How cybersecurity risk will be assessed and managed during the lifecycle
- Collaboration with the Authorizing Official to manage and maintain the system's cybersecurity risk posture

The PM develops the Cybersecurity Strategy. (Chief Engineer/Lead Systems Engineer/SSE, Chief Developmental Tester [CDT], ISSM)

- Is the Cybersecurity Strategy coordination maintained and configuration controlled with other governing program documents (SEP, PPP, ISP, ICD/CDD/CPD/CONOPS/capability requirements, Acquisition Strategy, RFPs)? The Acquisition Strategy should reference the Cybersecurity Strategy and outline key cybersecurity considerations that will affect the acquisition (including procurement), such as cybersecurity technical, cost, funding, staffing and support considerations. The SEP should also identify cybersecurity as an important design consideration and reference the Cybersecurity Strategy as a source for determining requirements. The ISP also relies on the program's Cybersecurity Strategy to determine compliance with DoD information management policies and compliance with the Global Information Grid architecture. The Cybersecurity Strategy and RMF assessment/authorization activities are aligned with the TEMP. (PM, Chief Engineer/Lead Systems Engineer/SSE, ISSM and Chief Developmental Tester)

- Have the Cybersecurity Strategy, SEP, TEMP, PPP, ISP, ICD/CDD/ CPD/CONOPS/capability requirements, Acquisition Strategy, and RMF Security Plan informed the RFP throughout the lifecycle? (Chief Engineer/Lead Systems Engineer, CDT, ISSM, Engineering/Systems Engineering [including program protection/SSE representative], Acquisition, T&E, and Cybersecurity WIPT leads)

- Was preference given to the acquisition of COTS cybersecurity and cybersecurity-enabled products, which have been evaluated and validated as appropriate, to be used on systems entering, processing, storing, displaying, or transmitting national security information? (ISSM)

- Are current cybersecurity threats included in the PPP threat table? (Chief Engineer/Lead Systems Engineer/SSE, ISSM)

- Is cybersecurity included in the program budget? Cybersecurity should be included as an identifiable line in the budget. When constructing the cybersecurity budget requirement, consider cybersecurity staff and support costs, cybersecurity SE costs, cybersecurity procurement costs, RMF authorization costs, cybersecurity T&E costs, and cybersecurity maintenance costs (from responding to IAVAs, etc., to maintaining cybersecurity posture during sustainment until decommissioning). Cybersecurity resources will require funding through various types of appropriations, since cybersecurity is considered throughout the full lifecycle of the program. For example, Research, Development, Test, and Evaluation funds are required for the DT&E of a cybersecurity solution. Procurement funds are required for

procurement of cybersecurity solutions or tools. Operations and Maintenance funds are required for the post-fielding operational maintenance of the cybersecurity posture, such as IAVA fixes. (Chief Engineer/Lead Systems Engineer/SSE, CDT, Program Lead, Business Financial Manager, Product Support Manager [Program Lead Logistician], Program Lead, Cost Estimator)

- After an ATO, is the system or information environment being continuously monitored for cybersecurity-relevant events and configuration changes that negatively impact cybersecurity posture, and are the quality of security controls implementation periodically assessed against performance indicators such as cybersecurity incidents, feedback from external inspection agencies, exercises, and operational evaluations? The ISSM may recommend changes or improvement to the implementation of assigned security controls, the assignment of additional security controls, or changes or improvements to the design of the system itself. Site operations staff and the ISSM are responsible for maintaining an acceptable level of residual risk. This is done by addressing cybersecurity considerations when changes are made to either the security controls baseline or to the baseline of the operational computing environment. The ISSM is responsible for determining the extent to which a change affects the cybersecurity posture of either the system or the computing environment, obtaining approval of cybersecurity-relevant changes, and documenting the implementation of that change in the Security Plan, POA&M, and site operating procedures. Continuous monitoring and periodic reviews ensure the system continues to comply with the cybersecurity requirements, current threat assessment, and CONOPS. Reviews are conducted at intervals predefined in the system-level continuous monitoring strategy. (ISSM, SSE)

- Is software authorized and the current approved version with cybersecurity patches and service packs installed? These are common issues that lead to attacks and intrusions. (ISSM)

L.4 Information Systems and IT Products

DoD information systems are authorized for operation through the full RMF process. Products are not authorized through the RMF process. However, products must be securely configured in accordance with applicable DoD policies and security controls and undergo special assessment of their functional and security-related capabilities and deficiencies.

Products (including applications) are defined in DoDI 8500.01 as “individual IT hardware or software items.” They can be commercial or government provided and can include, for example, operating systems, office productivity software, firewalls, and routers.

Information systems are composed of IT products. Tables 9, 10, and 11 illustrate the relationship between types of information systems and IT products.

Table 9. Relationship between Types of Information Systems and IT Products

Information System	Associated IT Product
Enclave	Routers, switches, firewalls, load balancers, IDS/IPS, wireless access points, network appliances, etc.
Major Application	Servers, operating systems, productivity software, mobile code, mobile apps, widgets, database management systems (DBMSs), storage devices, sensor agents, etc.

In the above examples, the IT system would go through the RMF process for an ultimate ATO decision. The individual IT products undergo a cybersecurity assessment. These examples are not to be construed as all-inclusive.

Products are configured in accordance with applicable Security Technical Implementation Guides (STIGs) under a cognizant ISSM and SCA. STIGs are product-specific and document-applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 (currently Revision 4) security controls into single, actionable, measurable items. Security Requirements Guides (SRGs) are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used. STIGs, SRGs, and CCIs are available on the IA Support Environment website (http://iase.disa.mil). STIG and SRG compliance results for products will be documented as security control assessment results within a product-level SAR and reviewed by the responsible ISSM (under the direction of the authorizing official) prior to acceptance or connection into an authorized computing environment (e.g., an IS or PIT system with an authorization). This review is to ensure products will not introduce vulnerabilities that the hosting IS cannot mitigate when incorporated or connected. DoD Component-level guidance maximizes the acceptance and reuse of testing and review results for widely used products to minimize duplication of effort across the DoD.

Table 10. DoD Information Systems and PIT Systems (Assess & Authorize)

DoD Information Systems and PIT Systems (Assess & Authorize)		
PIT System	**Enclave**	**Major Application**
Navy Ship	Navy Enterprise (e.g., Next Generation Enterprise Network)	Command and Control application (family of Global Command and Control System programs)
Tactical Weapons System	Air Force Intranet Increments	Defense Business Systems (family of Integrated Personnel and Pay System programs, Navy Enterprise Resource Planning, DoD Healthcare Management System Modernization program)

DoD Information Systems and PIT Systems (Assess & Authorize)		
PIT System	**Enclave**	**Major Application**
Combat Aircraft	Army LandWarNet	Global Combat Support System-Joint Increments
Tactical Vehicles		Acquisition Category (ACAT) III application programs
Industrial Control Systems	ICS Platform Enclave	Life Safety and Security Systems; Utility Monitoring and Control Systems

Table 11. Other DoD -IT (Assess Only)

Other DoD IT (Assess Only)		
PIT	**IT Services**	**Products**
See Table 12	IT services are outside the service user organization's authorization boundary, and the service user's organization has no direct control over the application or assessment of required security controls.	Routers, switches, firewalls, load balancers, intrusion detection systems/intrusion prevention systems, wireless access points, network appliances, etc.
	Internal IT services are delivered by DoD ISs	Servers, operating systems, productivity software, mobile code, mobile apps, widgets, database management systems, storage devices, sensor agents, etc.
	DoD organizations that use external IT services provided by a non-DoD federal government agency	
	DoD organizations that use external IT services provided by a commercial or other non-federal government entity	
	DoD organizations contracting for external IT services in the form of commercial cloud computing services	

L.5 Platform Information Technology (PIT) and Platform Information Technology Systems[59]

Platform information technology (PIT) and PIT systems are depicted in Figure 18. PIT may consist of both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems (i.e., platforms). PIT differs from

[59] Programs should refer to the RMF Knowledge Service for the most up-to-date information on PIT.

products in that it is integral to a specific platform type as opposed to being used independently or to support a range of capabilities (e.g., major applications or enclaves).

Owners of special-purpose platforms, in consultation with an authorizing official, may determine that a collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support. PIT systems are designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an authorizing official specifically appointed to authorize PIT systems.

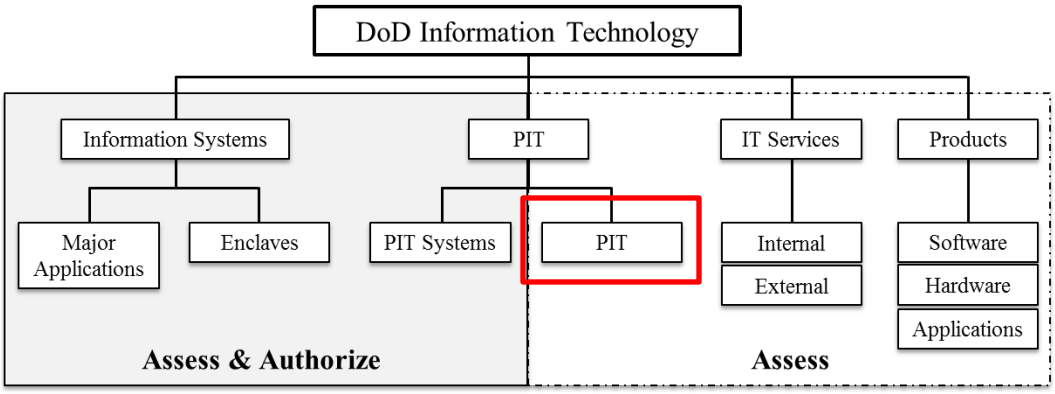


Figure 18. PIT and PIT Systems

All PIT has cybersecurity considerations, but PIT that does not rise to the level of a PIT system is not authorized for operation through the full RMF process. However, cybersecurity requirements are identified, tailored appropriately, and included in the acquisition, design, development, DT&E and OT&E, integration, implementation, operation, upgrade, or replacement of all DoD PIT. The ISSM (with the review and approval of the responsible authorizing official) is responsible for ensuring all PIT has completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

Interconnections between PIT systems and other PIT systems or DoD ISs are protected by implementation of security controls on either the PIT system or the DoD IS. For PIT systems that are stand-alone, assigned security control sets may be tailored as appropriate with the approval of the authorizing official (e.g., network-related controls may be eliminated).

PIT may be categorized using CNSSI 1253, with the resultant security control baselines tailored as needed. Otherwise, the specific cybersecurity needs of PIT are assessed on a case-by-case basis and security controls applied as appropriate. As required for products, compliance results for PIT should be documented as security control assessment results. These results are documented within a PIT-level SAR and reviewed by the responsible ISSM (under the direction of the authorizing official) prior to acceptance or connection to an authorized computing environment (e.g., an IS or PIT system with authorization).

PIT systems may also include other PIT systems (systems-of systems-concept) as well as PIT. Table 12 provides examples of PIT systems and associated PIT.

Table 12. Examples of PIT Systems and Associated PIT

PIT System	Associated PIT
Navy Ship	Command and Control, Fire Control, Radars, Test and Maintenance Equipment, etc.
Tactical Weapons System	Tactical Command System, Communication System, Radars, Launching System, etc.
Combat Aircraft	Avionics, Missile Systems, Electronic Warfare Modules, Radars, Communications, Displays, etc.
Tactical Vehicles	Power Generation and Distribution, Onboard Computer and Storage Systems, Tactical Radios, Vehicle Diagnostics, etc.
Industrial Control Systems	Life Safety and Security Systems; Utility Monitoring and Control Systems

In the above examples, the PIT system would go through the RMF process for an ultimate ATO decision. The individual PIT components undergo a cybersecurity assessment. This example is not to be construed as all-inclusive.

Other examples of PIT include:

- Application-specific integrated circuit modules.
- Training simulators.
- Diagnostic test and maintenance equipment.
- Calibration equipment.
- Equipment used in the research and development of weapon systems.
- Medical devices and health information technologies.
- Buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.).
- Utility distribution systems (such as electric, water, wastewater, natural gas, and steam).
- Telecommunications systems designed specifically for industrial control systems, to include supervisory control and data acquisition.
- Direct digital control, programmable logic controllers.
- Other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).

Annex M - Examples of Risk Management Framework (RMF) Implementation

M.1 Example 1 — Unmanned Aerial Bomber System (UABS)

M.1.1 Introduction

Purpose: Provide an example of a Platform Information Technology (PIT) system undergoing the RMF process.

References:

a) DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*
b) CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*
c) NIST SP 800-30, *Guide for Conducting Risk Assessments*
d) NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach*
e) NIST SP 800-39, *Managing Information Security Risk - Organization, Mission, and Information System View*
f) NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
g) NIST SP 800-60, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*
h) NIST SP 800-60, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*
i) NIST SP 800-82, *Industrial Control Systems Security Guide*
j) NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
k) NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems - Building Effective Security Assessment Plans*
l) *Department of Defense (DoD) Cybersecurity Risk Assessment Guide*

Background: Reference (a) provides DoD policy and the process for performing the RMF on all DoD information technology (IT); however, Reference (a) leverages the policy and processes in References (b) through (j). This example progresses through each of the RMF steps and tasks as described in Reference (d).[60] The six RMF steps are as follows, and the tasks supporting each step will be listed as each step is discussed below:

Step 1: Categorize System

Step 2: Select Security Controls

Step 3: Implement Security Controls

[60] See the summary chart of the RMF steps and tasks in Appendix E of Reference (d).

Step 4: Assess Security Controls

Step 5: Authorize System

Step 6: Monitor Security Controls

The example system is an unmanned aerial bomber system, which is a type of PIT system. This example was chosen because it offers the opportunity to examine less understood nuances of the RMF as they apply to PIT systems. The example will not document every detail of the RMF process, as the intent is simply to help program managers understand the fundamental concepts of the RMF and get them started on each step/task. For example, tailoring is an important concept for PIT systems. A few illustrative examples of such tailoring are provided. The discussions below are intentionally concise and are provided for illustrative purposes. For a more thorough discussion of each step/task, see Reference (d).

M.1.2 Step 1: Categorize System [per Reference (b)]:

Task 1-1. Security Categorization: Categorize the system and document the results of the security categorization in the Security Plan.

Reference (b) states that security categorization is a two-step process:

1. Determine potential impact values for the information types processed, stored or transmitted or protected by the system; and for the system.
2. Identify overlays that apply to the system and its operating environment to account for additional factors (beyond impact) that influence the selection of security controls.

To categorize the system, you must understand the mission as well as the information types and systems/networks used. The mission is to fly the unmanned aerial bombers to a target and drop bombs to destroy those targets. To execute the mission, air tasking orders are issued using a ground-based information system. The unmanned aerial bomber is remotely controlled and operated using a ground-based system. The bomber includes IT components that are essential to real time operation of the bomber itself – the IT is essential to loading air tasking orders, flying the aircraft, guiding it to its target, commanding it to release bombs, etc. The following table captures the impact values for each information type, which are rolled up into a high water mark for a system categorization, and it indicates the information owner for each information type used by the system.

Table 13. Information Type Impact Values

Information Type	Provisional Impact Values			Information Owner (Rank/Grade, Name, Org/Office Symbol)
	C	I	A	
Intelligence	H	H	M	[intelligence community]
Weather	L	M	M	[weather agency]
Logistics	M	H	H	[supply organization]
Personnel	L	M	M	[personnel organization]
Air Tasking Orders	H	H	H	[mission owner]
…				
System Information	H	H	H	[system owner]
System Categorization	H	H	H	

The mission owner owns the air tasking order. The air tasking order is generated using various information types, not all of which are actually owned by the mission owner or the system owner. The mission owner, in some cases, might not even own all systems used to execute the mission. As such, the program manager for the unmanned aerial bomber system must reach out to each information owner to determine the level of protection required for the individual information types.

Typical information types and their impact values are captured in Reference (g), and Reference (h) explains the concept of and setting of impact values. The information types used by national security systems may not be included in Reference (h); therefore, system owners and information owners may consult Reference (g) to determine how to set impact values, and the may also examine similar information types in Reference (h) in setting impact values for unique information types.

The intelligence community owns intelligence information the mission owner needs, such as where the targets are, if they're on the move, and how close to friendly forces they are. For the mission owner, the weather agency can predict the weather over the target on any given day, with a certain level of accuracy that decreases as the projection period increases. Supply organizations provide information on the availability of essential items, such as bombs and spare parts used by the bomber. Personnel organizations advise on the availability and readiness of key personnel, such as pilots (who fly the bomber from the ground) or maintenance personnel who prepare the bomber for its missions. System information types refer to the information necessary to operate the systems/networks (e.g., router tables, firewall rules, system configurations) and that must be protected, possibly to the highest level of the information processed by the system.

The impact values for each information type are expressed as low, moderate, or high for each security objective of confidentiality, integrity, and availability. The system categorization is a high water mark across information types, but not across security objectives. The distinct impact values (low, moderate, or high) to C-I-A for each information type are included in the Initial Capabilities Document (ICD) or Problem Statement. These information type impact values are constraints to each of the alternatives studied in the AoA. System categorization information may be captured in a template available on the RMF Knowledge Service at: https://rmfks.osd.mil/. This template helps program managers ensure all information types are identified and coordinated with the appropriate information owners. It may also be used to provide evidence to the Authorizing Official (AO) that program managers reached out to each information owner; signatures may be obtained from each information owner who coordinates on a "categorization memo" to the AO.

The system categorization must be documented in the system's Security Plan, which will be approved by the AO. The system categorization is also part of the Cyber Survivability/cybersecurity requirements of the System Survivability KPP documented in the Capability Development Document (CDD)/Capability Production Document/equivalent capability requirements document. It is advisable for program managers to get an early AO approval of the categorization, as it drives all other activities in the RMF process. Categorizing the system too high potentially wastes resources, and categorizing the system too low does not adequately protect the information and jeopardizes the mission.

All overlays that are applicable must be identified by the mission owner with support from the PM at this point, but they are not yet applied (i.e., no security controls tailoring takes place at this point based on the overlay specifications). Overlays are posted on the CNSS website at https://www.cnss.gov/CNSS/index.cfm as attachments to Appendix F of Reference (b). Each overlay includes a section to help determine the applicability of the overlay. The following table indicates which of the available overlays are applicable to the unmanned aerial bomber system (UABS).

Table 14. Applicable Overlays

Overlay Title	**Applicable to UABS**
Space Platform Overlay	No (but, command and control (C2) of UABS is similar to C2 of space platforms)
Cross Domain Solution (CDS) Overlay	Possibly (depends on system design choices)
Intelligence Overlay	Yes (assuming certain system design choices)
Classified Information Overlay	Yes

NOTE: NIST SP 800-82 Industrial Control Systems Security Guide Appendix G ICS Overlay should be used to address the supporting infrastructure (utilities, life safety and security systems, airfield and pier systems, etc.) required for the UABS mission support.

Following are examples of the tailoring of controls recommended by the overlays and the rationale for doing so. No examples are included from the Intelligence Overlay, because they are all For Official Use Only (FOUO). Again, the relevance of each recommendation below depends on the architecture of the system, and where the information types flow. For example, the bomber may not require security controls related to the CDS, if the architecture places that cross domain function solely within the ground systems. Conversely, the examples under the Space Platform Overlay likely apply to the bomber, but “bomber” could be substituted for “space platform” in most places below.

The security control identifiers (ID) and family names are contained in the table below.

Table 15. Security Control Identifiers and Family Names

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Space Platform Overlay Examples:

AU-7, Audit Reduction and Report Generation

Space Supplemental Guidance: Audit review and reduction is not performed directly on the space platform; rather, it is performed on audit data off-loaded to the ground segment. Reduction of audit data may occur on the space platform within the telemetry stream between the space platform and the ground. During anomaly resolution, this audit data can be modified to delve into specific points of interest within the space platform to aid in determining, identifying, and correcting system failures.

PE-4, Access Control for Transmission Medium

Space Supplemental Guidance: The threat addressed by this control is physical access to wired information system distribution and transmission lines. Such lines do not exist for the space platform; all communication is wireless.

ICS Overlay Examples:

PE-3, Physical Access Control

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

PE-11, Emergency Power

ICS Supplemental Guidance: Emergency power production, transmission, and distribution systems are a type of ICS that are required to meet extremely high performance specifications. The systems are governed by international, national, state, and local building codes, must be tested on a continual basis, and must be repaired and placed back into operations within a short period of time. Traditionally, emergency power has been provided by generators for short to mid-term power (typically for fire and life safety systems, some IT load, and evacuation transport) and uninterruptible power supply battery packs in distribution closets and within work areas to allow some level of business continuity and for the orderly shutdown of non-essential IT and facility systems. Traditional emergency power systems typically are off-line until a loss of power occurs and are typically on a separate network and control system specific to the facility they support. New methods of energy generation and storage (e.g., solar voltaic, geothermal, flywheel, microgrid, distributed energy) that have a real-time demand and storage connection to local utilities or cross connected to multiple facilities should be carefully analyzed to ensure that the power can meet the load and signal quality without disruption of mission essential functions.

Control Enhancement: (1) No ICS Supplemental Guidance.

Rationale for adding control to baseline: ICS may support critical activities which will be needed for safety and reliability even in the absence of reliable power from the public grid.

Cross Domain Solution Overlay Examples:

AC-4, Information Flow Enforcement

CDS Supplemental Guidance: Apply flow control to data transferred between security domains by means of a set of hardware and/or software collectively known as the "filter". Flow control includes the inspection sanitization, and/or rejection of data from one security domain prior to transfer of data to a different security domain. For an access CDS, the remote desktop architecture provides the capability for a user to have access from a single device to computing platforms, applications, or data residing on multiple different security domains; while preventing any information flow between the different security domains.

AC-6, Least Privilege

CDS Supplemental Guidance: The principle of least privilege for CDS extends to the sanitization of data prior to processing subsequent data transfers destined for a different security domain, thus precluding inadvertent access. Additionally, processes running on the CDS are not allowed access to the network if the access is not explicitly required for functionality, (e.g., a firewall is used to control access to and from the CDS).

Classified Information Overlay Examples:

AU-12, Audit Generation

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, requires agencies to monitor and audit user activity on classified networks. Generating audit records supports the detection of insider threat activities.

Regulatory/Statutory Reference(s): EO 13587, Sec 2.1(b) and Sec 5.2; White House Memorandum, National Insider Threat Policy, Tab 1, Sec B.2(1) and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Sec H.1.

MP-4, Media Storage

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Physically controlling and securely storing media is necessary to protect the classified information contained within the media.

Parameter Value: Physically controls and securely stores digital and non-digital media containing classified information within an area and/or container approved for processing and storing media based on the classification of the information contained within the media.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); CNSSP No. 26.

Task 1-2. System Description: Describe the system (including system boundary) and document the description in the security plan.

Descriptive information about the system is documented in the system identification section of the SP, included in attachments to the plan, or referenced in other standard sources for information generated as part of the system development lifecycle. Duplication of information is avoided, whenever possible. The level of detail provided in the SP is typically commensurate with the security categorization of the system. The RMF KS provides a template for the security authorization package, which includes the SP. That SP template includes pre-defined fields the program manager or representative (normally the ISSM) must fill in. A sampling of the fields in the template follows:

System Name:	Unmanned Aerial Bomber System
System Acronym:	UABS
System Identification:	[unique ID, generated from Enterprise Information Technology Data Repository (EITDR)]
System Type:	Platform IT System
System Lifecycle/Acquisition Phase:	Pre-Milestone A
Version/Release #:	1.0
DoD Component:	Air Force
Port, Protocol, Service Management (PPSM) Registry Number:	[unique ID from PPSM registry]
System Location:	Multiple Locations
Type Authorization:	Yes
Physical Location:	Fixed ground stations deployed at [???] HQ Central Command; mobile unmanned aerial bombers deployed at [???] forward combat locations
System Description:	Large platform unmanned aerial bomber flown remotely from ground stations to deploy smart bombs (up to 500 pounds) to selected targets for destruction.

Software Category:	GOTS
Mission Criticality:	Mission Critical (MC)

Task 1-3. System Registration: Register the system with appropriate organizational program/management offices (e.g. DoD Information Technology Portfolio Registry (DITPR), EITDR).

All Air Force systems must be registered in the Air Force EITDR, and information systems must be subsequently registered in the DITPR. In this example, the bomber itself is platform IT, but the ground systems used to generate the air tasking orders and to fly the bomber are not necessarily platform IT. As such, the overall system may need to be registered in EITDR and DITPR. Program managers are advised to confer with their EITDR and DITPR points of contact to determine if registration is required for which system components. A unique identifier is associated with each EITDR or DITPR entry, and that identifier is included in the "System Identification" field in the security plan. All Air Force systems must also be entered into Enterprise Mission Assurance Support System (eMASS), which automates the RMF process workflow, among other things. Other DoD Components may also require use of eMASS.

M.1.3 Risk Management Framework Step 2: Select Security Controls

Task 2-1. Common Control Identification: Identify the security controls that are provided by the organization as common controls for organizational systems and document the controls in a SP.

The unique environment within which the UABS operates and the corresponding architecture drive which controls are common and can, therefore, be inherited by the system. The overall UABS is designed within the context of that architecture, either to take advantage of existing common controls or to avoid the risk imposed by interconnecting to systems/networks providing common controls, but that ultimately have interconnectivity to the Internet, to which all threat actors have access. The more unique the system, the less well it may fit within the typical information system/network/enterprise architecture. The bomber is unique as compared to typical information systems, but the supporting ground systems are very much like typical information systems. However, the ground systems' degree of separation from NIPRNet and SIPRNet where common controls are provided may reduce the degree of inheritance of those common controls and, thereby, increase the burden of developing and providing such controls within the bomber and its supporting infrastructure.

In this example, for the bomber itself, the concept of a typical information system in a fixed facility does not apply. As such, we must consider which controls or families of controls can be tailored out before we can determine which controls remain and, of those, which can be inherited from a common control provider. For example, while the bomber is on the ground, it can inherit the protection from security controls such as: the base perimeter fence, gates, and guards; base-wide security patrols from the Security Forces; flight line or hanger perimeter fences/structures, outside lighting, and security patrols; fire detection/suppression in the hanger (not on the bomber). But while the bomber is in flight, such ground-based concepts do not apply. However,

other forms of physical protection could apply, such as anti-tamper and/or cryptographic zeroization, in case the bomber crashes in enemy territory and is seized by the enemy. Tailoring of such controls is discussed below. Other inheritable controls may include cryptographic key management infrastructure, bulk encryption of communications lines (those used to command and control the bomber), and monitoring for and response to network-based attacks against any of the IT used in or to communicate with the bomber. Potentially inheritable security controls include, but are not limited to:

- PE-1, Physical and Environmental Protection Policy and Procedures
- PE-2, Physical Access Authorizations
- PE-3, Physical Access Control
- PE-6, Monitoring Physical Access
- PE-8, Visitor Access Records
- PE-9, Power Equipment and Cabling
- PE-13, Fire Protection
- SC-12, Cryptographic Key Establishment and Management

In this example, for the ground-based system components, the entire boundary protection suite (firewalls, intrusion detection/prevention systems, network account management and access control, etc.) may be inherited from the hosting base enclave, assuming all stakeholders agree the risk imposed by connecting to such base enclaves is acceptable (this is a risk-based design decision based on systems security engineering (SSE), which is part of the standard systems engineering (SE) process used during the acquisition lifecycle). The security capability requirements (e.g., system survivability KPP cyber survivability and cybersecurity requirements), CONOPS, mission threads, architecture design flows, and SSE risk assessments, mitigations, and design trades drive the definition of security technical requirements included in the technical configuration baselines: functional, allocated, and product. Security controls (informally grouped into technical, management, and operational controls) map to technical requirements in specifications (part of the functional, allocated, and product baselines), process, and personnel requirements. Most of the physical and environmental controls are also inherited, such as: base perimeter fence, gates, and guards; base-wide security patrols from the Security Forces; facility perimeter fence, outside lighting, and security patrols; internal facility guards, checkpoints, security cameras, intrusion detection systems, and alarm systems; facility fire detection and suppression systems; facility temperature and humidity controls, awareness and training, etc. Potentially inheritable security controls include, but are not limited to[61]:

- AC-1, Access Control Policy and Procedures
- AC-2, Account Management
- AC-17, Remote Access
- AT-1, Security Awareness and Training Policy and Procedures
- AT-2, Security Awareness Training
- AU-1, Audit and Accountability Policy and Procedures
- AU-2, Audit Events

[61] Most of the "dash-1" controls are inheritable, as they require policies and procedures most often developed by the organization, at a level higher than the development, acquisition, or operating organizations.

- AU-6, Audit Review, Analysis, and Reporting
- AU-7, Audit Reduction and Report Generation
- PE-1, Physical and Environmental Protection Policy and Procedures
- PE-2, Physical Access Authorizations
- PE-3, Physical Access Control
- PE-6, Monitoring Physical Access
- PE-8, Visitor Access Records
- PE-9, Power Equipment and Cabling
- SC-1, System and Communications Protection Policy and Procedures
- SC-7, Boundary Protection
- SC-8, Transmission Confidentiality and Integrity
- SC-12, Cryptographic Key Establishment and Management
- SC-13, Cryptographic Protection
- SC-17, Public Key Infrastructure Certificates
- SC-20, Secure Name /Address Resolution Service (Authoritative Source)
- SC-38, Operations Security

For the bomber and the supporting ground components, many "management" security controls (i.e., organizational cybersecurity program functions or RMF process-oriented functions) and "operational" security controls (i.e., those performed by the operational community or RMF people-oriented functions) are inheritable, such as those associated with establishing and performing the security controls assessment and authorization of the system, and those associated with maintaining the cybersecurity posture over time (i.e., monitoring and computer network defense). Potentially inheritable security controls include, but are not limited to:

- CA-1, Security Assessment and Authorization Policies and Procedures
- CA-2, Security Assessments
- CA-6, Security Authorization
- IR-1, Incident Response Policy and Procedures
- IR-4, Incident Handling
- IR-5, Incident Monitoring
- IR-7, Incident Response Assistance
- IR-9, Information Spillage Response
- RA-1, Risk Assessment Policy and Procedures
- RA-3, Risk Assessment

Task 2-2. Security Control Selection: Select the security controls for the system and document the controls in the SP.

Reference (b) states that security control selection is a two-step process:

1. Select initial security control set (i.e., baseline controls with any selected overlays applied).
2. Tailor initial security control set.

As described in Task 2-1, Common Control Identification, selection/tailoring is a risk- and mission-based process enabled by SSE and SE.

The system categorization drives the baseline set of security controls from Reference (b). Given there are three security objectives and each has three possible values, there are 27 possible baselines. The CNSSI 1253 baselines were originally developed against a set of assumptions that do not often apply to PIT systems or other non-information systems; therefore, significant tailoring of security controls is necessary for the bomber, but not so much for the supporting ground systems. Following are the assumptions from Reference (b), with notional indications of which assumptions apply to each component of the UABS.

Table 16. Assumptions

Assumptions	Apply to Bomber?	Apply to Ground Systems?
Information systems are located in physical facilities.	No	Yes
User data/information in organizational information systems is relatively persistent.	No	Yes
Information systems are multi-user (either serially or concurrently) in operation.	No	Yes
Some user data/information in organizational information systems is not shareable with other users who have authorized access to the same systems.	Yes	Yes
Information systems exist in networked environments.	No	Yes
Information systems are general purpose in nature.	No	No
Organizations have the structure, resources, and infrastructure to implement the controls.	Yes	Yes
Insider threats exist within NSS organizations.	Yes	Yes
Advanced persistent threats (APTs) are targeting NSS and may already exist within NSS organizations.	Yes	Yes

A baseline is simply a starting point, and tailoring of security controls is required for all systems. The less the system aligns with the assumptions used to generate the baselines, the more tailoring we must perform. Overlays are a form of bulk tailoring by a community who owns or has an interest in the type of system, information, or environment. More importantly, the overlays provide the rationale for selecting or de-selecting security controls, and that rationale is risk-based. As such, a risk assessment is necessary to determine if the UABS has (or will have, if not yet developed) vulnerabilities that may be exploited by various threat sources. If the baseline does not include security controls designed to mitigate the threat/vulnerability identified in the risk assessment, the control is selected and applied beyond the baseline. Conversely, if the baseline includes security controls designed to mitigate a threat/vulnerability the UABS does not or will not suffer, the security control may be de-selected. Risk assessments are performed during the system lifecycle at the times when the design maturity is assessed and a decision is made that a design is ready to move to the next level elaboration (i.e., requirements definition to

system-level design to preliminary design to detailed design to implementation (e.g., fabrication, coding, acquiring) to integration and test (verification and validation). These gates line up with the Systems Engineering Technical Reviews (SETRs) and other program/technical reviews (e.g., System Requirements Review, System Functional Review, Preliminary Design Review, Critical Design Review, Test Readiness Review, and System Verification Review).

It is mandatory to identify and use all appropriate overlays, but it is not mandatory to comply precisely with all specifications in all overlays, as even the overlays were developed based on a set of assumptions that may or may not apply to all systems using the overlay. That is, further tailoring of the overlay specifications is often required; this is system-specific tailoring, and the rationales for selecting or de-selecting the controls must be documented in the SP for Authorizing Official (AO) approval. The PM and chief engineer ensure controls they document in the SP map to technical requirements in specifications, process, and personnel requirements. Again, these are risk-based decisions that require a risk assessment with evidence the AO uses to make his or her decision.

In this example, the Classified Information Overlay is applicable, as intelligence information is processed, and the air tasking orders are likely classified. The Intelligence Overlay may be applicable, but possibly only to certain components of the systems. For example, the bomber itself may not need to process intelligence information, but the component of the system that ingests the intelligence information in order to create the air tasking order may need to apply the Intelligence Overlay. Depending on the environment in which the system operates, the corresponding architecture, and the design of the system (i.e., the interconnectivity selected), the Cross Domain Solution (CDS) Overlay may be applicable. The design may be such that a CDS (and its associated security controls) is avoided and instead an air gap is used. The bomber has many similarities to an unmanned space platform, such as the means of commanding and controlling the bomber, the hostile operating environment, the lack of normal identification and authentication methods; therefore, the security control specifications in the Space Platform Overlay may apply. To be clear, the overlay is not applicable, but the program manager may leverage some content. Be sure to examine the risk-based rationale (tied to system characteristics) for each security control selected or de-selected in the Space Platform Overlay to determine if it can be leveraged in tailoring the bomber's set of security controls.

Note that in this example, the program office may choose to pursue authorization of the bomber separately from the supporting ground systems. In fact, the supporting ground systems may be used to support multiple platforms; therefore, it may not be appropriate or advisable to establish the authorization boundary around all types/families of unmanned aerial vehicles and all supporting ground systems. Before the SP is drafted, PMs are advised to work with their AOs to determine the appropriate authorization boundaries. Another factor to consider in setting authorization boundaries is the size (and complexity) of the system authorized; too large, and we'd be constantly updating the authorization package to respond to changes impacting risk; too small, and it would be difficult to keep up with multiple packages and, more importantly, to consistently manage risk across systems. For the bomber in this example, while it is in flight, security controls associated with guns, gates, and guards; fire detection/suppression; temperature/humidity control; locking screen savers (because there are no screens); etc. may be tailored out, with a risk-based justification (i.e., the bomber does not suffer the

threat/vulnerability for which the control was designed to mitigate). Security controls for the bomber that may be tailored out include, but are not limited to:

- AC-7, Unsuccessful Logon Attempts
- AC-8, System Use Notification
- AC-9, Previous Logon (Access) Notification
- AC-11, Session Lock
- AC-12, Session Termination
- AC-22, Access Control for Mobile Devices
- MP-2, Media Access
- MP-3, Media Marking
- MP-4, Media Storage
- MP-5, Media Transport
- PE-2, Physical Access Authorizations
- PE-3, Physical Access Control
- PE-4, Access Control for Transmission Medium
- PE-5, Access Control for Output Devices
- PE-6, Monitoring Physical Access
- PE-8, Visitor Access Records
- PE-10, Emergency Shutoff
- PE-11, Emergency Power
- PE-12, Emergency Lighting
- PE-13, Fire Protection
- PE-15, Temperature and Humidity Controls
- PE-16, Delivery and Removal
- PE-17, Alternate Work Site
- SC-15, Collaborative Computing Devices
- SC-19, Voice Over Internet Protocol
- SC-23, Session Authenticity
- SI-8, Spam Protection
- SI-10, Information Input Validation

In addition to determining which security controls are not applicable to the bomber, we must also determine which controls may be implemented differently due to the unique system design, use, or operating environment. For example, it may be necessary to authenticate to the bomber in order to command and control it, but the bomber does not have the typical user accounts, for which the Identification and Authentication (IA) family of controls are designed. Therefore, the basic intent of the IA Family can be met, albeit by alternate implementations appropriate for the bomber. Security controls for the bomber in flight that may be implemented differently than intended for typical information systems include, but are not limited to:

- AC-17, Remote Access
- AC-18, Wireless Access
- AU-4, Audit Storage Capacity
- CM-11, User-Installed Software

- IA-2, Identification and Authentication (Organizational Users)
- IA-3, Device Identification and Authentication
- IA-4, Identifier Management
- PE-9, Power Equipment and Cabling
- PE-14, Temperature and Humidity Controls

Alternative implementations (to meet the intent) of the controls listed immediately above are examples of mitigations to protect the system and information that would be identified as mitigations to a SSE risk- and mission-based assessment of the system (including all interconnected and interfaced systems, including mission planning and ground support, and data flows).

Task 2-3. Monitoring Strategy: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the system and its environment of operation.

DoD will develop a continuous monitoring strategy per Reference (a) based on the concepts in Reference (i). However, just as the security control baselines were designed to address a typical information system, the DoD strategy will align with typical information systems. As such, the UABS system owner must examine any DoD or DoD Component guidance to determine which aspects require adjustment or specialized treatment in the UABS Information Security Continuous Monitoring Strategy.

Any system-level continuous monitoring strategy must address the criticality, method (manual vs. automated), and frequency of monitoring all security controls. The intent is to advise the AO if a security control becomes non-compliant, or rather is ineffective in mitigating risk. The strategy must address the reporting requirements and documentation provided to the AO, who decides whether or not to modify the authorization decision (e.g., no change, ATO becomes ATO with conditions, Denial of ATO).

It is necessary to draft the monitoring strategy at this point, as it quite possibly feeds the selection of security controls, and vice versa. That is to say, if a control cannot be monitored over time to determine effectiveness, there may be no need to implement the control, the control may need to be implemented differently, or the risk must be mitigated via compensating controls.

Given the UABS is a PIT system, it is likely its monitoring strategy will be adjusted significantly (compared to the DoD strategy, process, or guidance). For example, consider that most typical systems rely heavily on a Computer Network Defense Service Provider (CNDSP) (to become cybersecurity service provider) to monitor many of the technical security controls implemented on or provided to (as common, inherited controls) the UABS. (NOTE: Many security controls are designed solely to provide monitoring capabilities.) However, design decisions may dictate that the UABS be isolated from those CNDSPs residing on NIPRNet and SIPRNet. As such, the monitoring strategy must be aligned with the architecture of the supporting infrastructure and the system design. Knowing how security controls can and will be monitored actually drives the design of the system. If there are no available CNDSPs, the system or supporting infrastructure must be designed and implemented to provide monitoring services.

The system-level continuous monitoring strategy must align with the cybersecurity DT&E and OT&E sections of the Test and Evaluation Master Plan (TEMP), which documents test and evaluation of components, subsystems, and system level to verify security requirements in the specifications and capability requirements document are met and assess system vulnerabilities in a cyber threat environment. The TEMP will document plans for DoDI 5000.02-required cybersecurity DT&E, 1) The DT&E program will support cybersecurity assessments and authorization, including Risk Management Framework security controls, and 2) the Program Manager and Operational Test Agency will conduct periodic cybersecurity risk assessments to determine the appropriate Blue/Green/Red Team, and operational impact test events in alignment with the overall test strategy for evaluating the program for real world effects. Also, DOT&E's Core Cybersecurity Compliance Metrics are directly related to security controls. The metrics are the minimum compliance baseline to be verified during the cooperative vulnerability assessment and penetration testing phase. OT&E is conducted to validate the operational effectiveness, suitability, and survivability (including the cyber threat environment and cybersecurity).

Task 2-4. Security Plan Approval: Review and approve the security plan.

Program managers simply must engage with the AO early and often to ensure any assumptions about risk, architecture, requirements, design, implementation, etc., are valid and up-to-date. Failure to get agreement early on the SP jeopardizes the system's cost, schedule, and performance (i.e., it may not receive a timely ATO). The SP documents the categorization, security control baseline, and tailoring of security controls. Given the security controls map to system security requirements and system design, PMs ensure the AO (or designated representative) is involved in the review of the acquisition documentation that includes relevant cybersecurity information, and participates in SE/SSE/cybersecurity WIPTs, SETRs, and critical milestone decisions. It is essential the AO understands and accepts the risk inherent in the solution architecture, system requirements, and design to determine the derived corresponding set of security controls is acceptable. The AO approves the PM-provided SP.

If the SP is changed throughout the system lifecycle (and that is very likely given the iterative nature of system design for specialized systems), it is necessary to get another approval from the AO. This point is particularly relevant to the UABS, as it is a PIT system that may struggle through design iterations, as that design relates to presumed infrastructures, security architectures, service providers, and so on that may or may not be available or appropriate.

M.1.4 Risk Management Framework Step 3: Implement Security Controls

Task 3-1. Security Control Implementation: Implement the security controls specified in the security plan.

Security controls are not requirements in and of themselves. Security controls can be used to derive actual system security requirements, which state more specifically the functions, performance, and characteristics to protect the system and data, implement security features of the architecture, and satisfy security capability requirements (e.g., system survivability cyber resilience and cybersecurity requirements. As such, SSE is the critical to building cybersecurity into the system. The item detail specifications, part of the initial product baseline at the CDR SETR, is the build-to specification. The chief engineer and SSE contribute to development of the item detail specification.

Given the UABS is a PIT system, standard solutions designed for typical information systems may not be possible or appropriate for the UABS, particularly the bomber component. The threat/vulnerability for which the original security control was designed is present (that's why the control was selected), but the UABS design necessitates a specialized design and implementation of the control. If the SSE risk assessment confirms the architecture and design are secure and pose low risk to the mission, the item detail specifications, when implemented and integrated up to the system level, should result in a secure system and system performance specification to be verified during system developmental T&E.

The previous example of how the pilot authenticates to the bomber is relevant here. For example, the bomber may not have user accounts for authentication, but the means of communication (e.g., dedicated point-to-point "wireless" link with encryption) may fulfill the intent of identification and authentication security controls, in that only authorized pilots on the ground in a protected facility on a UABS system component can talk to and fly the bomber. Showing this tailored implementation, and more importantly the need to tailor, to the Security Controls Assessor, to any oversight organizations, and ultimately the AO is crucial for PIT systems, as they must understand how all risks (for which controls were selected) are actually mitigated.

Task 3-2. Security Control Documentation: Document the security control implementation, as appropriate, in the SP, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

The SP is updated throughout the system's lifecycle to document how the security controls are actually implemented. The SP can either include the details of implementation (especially if "standard," well-known solutions are used – less explanation is needed) or reference existing acquisition artifacts that provide those details. Given the unique nature of the UABS, it is likely more appropriate to reference detailed system acquisition artifacts; however, to facilitate assessments and authorization decisions, it is advisable to reference specific sections of existing artifacts.

The mandatory security authorization package consists of the SP, the Security Assessment Report (and inherently the Risk Assessment Report), and the Plan of Action and Milestones. These are the high-level, RMF-specific artifacts. But, as discussed above, there are many other artifacts (e.g., DT&E Assessment and OT&E report) that tend to prove the effectiveness of all implemented security controls. Many of these artifacts are generated as part of normal system acquisition/development, SSE, DT&E, and OT&E. To the maximum extent possible, leverage existing artifacts. Reference those artifacts in the SP, which is approved by the AO, which thereby implies those artifacts will be acceptable for assessments and for an authorization decision. Following are examples of artifacts that may be leveraged:

- Agreed Data Requirements List (ADRL)
- COMSEC Material Control Guide (CMCG)
- Conformance Test Plan (CTP)
- Conformance Test Report (CTR)
- Continuity of Operations Plan (COOP)
- Cross Domain Appendix (CDA)

- Cryptographic Concept of Operation (CCO)
- Fail-Safe Design Analysis (FSDA)
- Incident Response Plan/Tactics, Techniques and Procedures (IRP/TTP)
- Interface Requirements Specification (IRS)
- Interface Design Document (IDD)
- Key Management Description (KMD)
- Key Management Plan (KMP)
- Memorandum of Agreement (MOA)
- Operating Procedures (OP)
- Operational Configuration Management Plan (OCMP)
- Operational Concepts Description (OCD)
- Operational Requirements Document (ORD)
- Penetration Test Plan (PTP)
- Program and Budget Documentation (PBD)
- Software Development Plan (SDP)
- Software Installation Plan (SIP)
- Software Test Plan (STP)
- Software User's Manual (SUM)
- System Concept of Operations (CONOPS)
- System/Subsystem Detailed Design (SSDD)
- System/Subsystem Specification (SSS)
- TEMPEST Control Plan (TCP)
- TEMPEST Test Plan and Report (TTPR)
- Test and Evaluation Master Plan (TEMP)
- Theory of Compliance (TOC)
- Theory of Design and Operation (TDO)
- Version Description Document (VDD)
- Work Breakdown Structure (WBS)

M.1.5 Risk Management Framework Step 4: Assess Security Controls

Task 4-1. Assessment Preparation: Develop, review, and approve a plan to assess the security controls.

For PIT systems like the UABS, the typical assessment procedures provided on the RMF Knowledge Service may need to be tailored. This is so, because the more the implementation was tailored, the more the assessment of the implementation will be unique to the system. If the DoD assessment procedures are not appropriate, it may be beneficial to go back to the more generic assessment procedures in Reference (j) for ideas on how the security control implementation can be assessed.

The TEMP documents plans for 1) DT&E of components, subsystems, and system level to verify security requirements in the specifications, 2) OT&E of the system to validate capability requirements documents are met, 3) assessment of system vulnerabilities in a cyber threat environment, among other cybersecurity objectives. The TEMP will document plans for DoDI 5000.02-required cybersecurity DT&E including vulnerability and adversarial cybersecurity test

and evaluation. The DT&E program will support cybersecurity assessments and authorization, including Risk Management Framework security controls. The Program Manager and Operational Test Agency will conduct periodic cybersecurity risk assessments to determine the appropriate Blue/Green/Red Team, and operational impact test events in alignment with the overall test strategy for evaluating the program for real world effects. Also, DOT&E's Core Cybersecurity Compliance Metrics are directly related to security controls. The metrics are the minimum compliance baseline to be verified during the cooperative vulnerability assessment and penetration testing phase. OT&E is conducted to validate the operational effectiveness, suitability, and survivability (including the cyber threat environment and cybersecurity).

This example below of the DoD implementation guidance and assessment procedures reveals how they may need to be tailored for the UABS, especially considering the notion of "automatically compliant" – it assumes a certain infrastructure is in place. Consider also that the bomber component of the UABS likely has size, weight, and performance constraints that may not allow traditional cybersecurity solutions (e.g., robust audit trails) to be implemented. Auditing is crucial to the monitoring capability, but if auditing cannot be implemented as intended, compensating controls may be implemented. When the blue highlighted assignment values are not specified in the DoD-specific assignment values (DSPAVs), the DoD Component or the system owner must determine the appropriate values and correspond to performance values in the specifications. Because this example security control is associated with monitoring, it affects the continuous monitoring strategy, and as such the assignment values may influence the monitoring frequency in the strategy. Note also that this example correlates to the need to determine who or what provides the CNDSP services (i.e., what is meant by "The organization" at the beginning of the control text), which is not a trivial task for the UABS, particularly the bomber component.

Control Number/Name: SI-4, Information System Monitoring

Control Text: The organization:

a. Monitors the information system to detect:

    1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and

    2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];

c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

DoD-Specific Assignment Value (DSPAV):

a. (1) sensor placement and monitoring requirements within CJCSI 6510.01F

b. (2) not appropriate to define at the Enterprise level

c. (1) not appropriate to define at the Enterprise level

d. (2) not appropriate to define at the Enterprise level

e. (3) not appropriate to define at the Enterprise level

Table 17. Applicable CCIs

Control Correlation Identifier (CCI) and Text	Implementation Guidance	Validation Procedures
CCI-001253: The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization being inspected/ assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.
CCI-002641: The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F. The organization must maintain an audit trail of monitoring. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F.
CCI-002642: The organization monitors the information system to detect unauthorized local connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized local connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized local connections.
CCI-002643: The organization monitors the information system to detect unauthorized network connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized network connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized network connections.
CCI-002644: The organization monitors the information system to detect unauthorized remote connections.	The organization being inspected/assessed documents and implements a process to monitor information system to detect unauthorized remote connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized remote connections.
CCI-002645: The organization defines the techniques and methods to be used to identify unauthorized use of the	The organization being inspected/assessed defines and documents the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques and methods to be used to

Control Correlation Identifier (CCI) and Text	Implementation Guidance	Validation Procedures
information system.	methods are not appropriate to define at the Enterprise level.	identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.
The organization identifies unauthorized use of the information system through organization-defined techniques and methods	The organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645. The organization must maintain an audit trail of identified instances of unauthorized use.	The organization conducting the inspection/assessment obtains and examines the audit trail of identified instances of unauthorized use to ensure the organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645.

The CCI list, as well as the process and specification, can be found on DISA's Information Assurance Support Environment site at: http://iase.disa.mil/stigs/cci/Pages/index.aspx. CCIs provide standard identifiers and descriptions for each of the singular, actionable statements comprising a security control or cybersecurity best practice. CCIs bridge the gap between high-level policy expressions and low-level technical implementations. CCIs allow a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control. This ability to trace security requirements from their origin (e.g., regulations, cybersecurity frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple cybersecurity compliance frameworks. CCIs also provide a means to objectively rollup and compare related compliance assessment results across disparate technologies.

Below is an extract from Reference (j), which takes a different, more generic approach. Even so, it too can provide ideas on how to assess this same example control.

SI-4, Information System Monitoring

Potential Assessment Methods and Objects:

Examine: [SELECT FROM: Continuous monitoring strategy; system and information integrity policy; procedures addressing information system monitoring tools and techniques; facility diagram/layout; information system design documentation; information system monitoring tools and techniques documentation; locations within information system where monitoring devices are deployed; information system configuration settings and associated documentation; other relevant documents or records].

Interview: [SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information

system; organizational personnel with responsibility monitoring the information system].

Test: [SELECT FROM: Organizational processes for information system monitoring; automated mechanisms supporting and/or implementing information system monitoring capability].

Task 4-2. Security Control Assessment: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

The RMF's intent is to integrate or synchronize the security assessment plan with the TEMP. We cannot assess cybersecurity capabilities separately from other functionality, as a change to one function to address a weakness may negatively impact another function. It must be a comprehensive assessment, which is especially critical for PIT systems where the IT is essential to real time operation of the platform. That is, if the IT (flight control system) fails on the bomber, it crashes. No changes to the security controls implementation can be made without considering the impact on the key functions of the bomber. As an extreme example, implementation of a timeout on the session which connects the pilot to the bomber would be catastrophic. Blindly implementing a timeout in response to an assessment indicating security control AC-12, Session Termination, is not compliant will jeopardize the mission, not to mention the safety and life of anyone under the bomber as it is crashing. Therefore, in developing the system and the security assessment plan, alternate means of terminating no longer needed "sessions" used to command and control the bomber must be designed, implemented, and assessed accordingly – assessment plans must match the implementation.

Given how system-specific the assessment of security controls on the bomber may be, it is advisable to ensure such assessments are incorporated into all phases of testing, to include DT&E. It would be beneficial to make it clear to the Security Controls Assessor in the Security Assessment Plan that the controls will be assessed iteratively during DT&E; however, the program manager is expecting the Security Controls Assessor, or their "Agent," to perform an independent analysis. Independence is critical to this assessment, and the Security Controls Assessor will indicate to all concerned what level of independence is required. The less knowledge the Security Controls Assessors have about specialized systems (e.g., the UABS), the more they may rely on DT&E to reveal weaknesses and simply perform an assessment on those DT&E results. Again, coordinate early with the Security Controls Assessors to determine how much any existing acquisition-based or SSE-based DT vulnerability and adversarial testing can be leveraged for security controls assessments.

Task 4-3. Security Assessment Report: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

This task is almost exclusively the responsibility of the Security Control Assessor; however, they may choose to leverage existing test results; therefore, the program office may be involved in preparing the report. Following are the fields included in the template for the security authorization package, which includes the Security Assessment Report. Explanations of each field are provided in that same template. A row is created in a spreadsheet to provide information in each of these fields for every non-compliant security control. Program offices

should be prepared to assist the Security Control Assessor in filling out some of these fields, in particular the NA justification and the recommendations for fixing the weakness.

- Security Control Number
- Security Subject Area (i.e., which family of security controls)
- Security Control / Enhancement Name
- Common Control Provider Information
- Overlay
- Compliant / Non-Compliant / Non-Applicable (C/NC/NA)
- NA Justification
- Vulnerability Summary
- Vulnerability Severity Value
- Security Control Risk Level
- Recommendations
- Last Update

The Security Control Assessor must perform a risk assessment of any non-compliant security controls. Although Reference (a) is not very clear about this fact, the Security Control Assessor must also prepare the Risk Assessment Report. But again, the assessor may not be familiar enough with specialized systems or PIT systems, such as this UABS example. Because of their deep knowledge of the system's functions, the program manager and supporting staff (e.g., system engineer, systems security engineer, Information System Security Manager (ISSM)) may need to work with the assessor on certain aspects of the Risk Assessment Report, such as determining the likelihood of a threat source initiating a threat event (e.g., an attack) against a vulnerability (e.g., a non-compliant security control) as well as the likelihood of success. And assuming the program office has worked with the operating community, they may also be able to advise the assessor of the mission impact due to any failure of the system (e.g., non-compliant security controls). The program office may leverage existing, acquisition or generic (i.e., non-RMF) risk models; cybersecurity can be incorporated into those models. Following are examples of how to capture and express the risk factors discussed above, and these examples resemble many generic models. Reference (k) and the RMF Knowledge Service explain each risk factor, how they are determined, and how they are used to generate a risk level.

Table 18. Likelihood of Threat Events

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Overall Likelihood

Table 19. Overall Likelihood and Level of Impact

Overall Likelihood	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Level of Risk (Combination of Likelihood and Impact)

In this UABS example, for the command and control "session" between the ground system and the bomber, let's assume security control AC-12 was selected, but it was not implemented; therefore, the security control assessment reveals the control is non-compliant. The task at hand is to determine the risk. The program office and the mission owner convey to the assessor that the likelihood of a session being left open and unattended for an indefinite period of time is not likely, as these "sessions" are initiated only while an air tasking order is being executed and the bomber is flying. In fact, an entire crew on the ground is used to execute the mission, and it would be intuitively obvious to the crew that the "session" was not gracefully terminated when the bomber landed. As such, the likelihood of an attacker high jacking a latent, unattended "session" is low (if not very low). If, however, the session was high jacked, the impact could be catastrophic (i.e., very high), as it would allow the attacker to take control of the bomber, fly it to a friendly target, and destroy that target. It may appear by plotting the likelihood and impact on the chart above that the risk would be Moderate. But, consider that there are other mitigating factors, such as the ability to shoot down the rogue bomber if the attacker in fact took control of it. Therefore, in the final analysis, the risk of this particular threat/vulnerability is assessed to be low. Such a risk is likely acceptable to the AO, but only if it can be shown how we arrived at the risk level – show the details of the risk assessment.

Note that per Reference (a), if the risk of any non-compliant security control is High or Very High, the authorization decision must be elevated to the DoD Component CIO. The CIO must explicitly allow the AO to issue an authorization decision.

Task 4-4. Remediation Actions: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

For PIT systems such as this UABS example, IT is embedded and early design decisions may be locked in, which may make it difficult to remediate any weaknesses identified during testing. As such, it is important to consider an iterative testing approach, persuading the Security Control Assessor to assess individual system components as they are being developed, so long as their implementation is relatively fixed and will be incorporated into the larger system. In this manner, early fixes are less impactful to the overall program cost, schedule, and performance. This is the same approach in which DT&E assesses the system to identify weaknesses/vulnerabilities, which should be appropriately mitigated via changes to the system architecture, requirements, design, and/or implementation. If high-risk weaknesses are identified during security control assessments, they must be addressed. Whether or not they can be addressed before the final Security Assessment Report is developed is the concern here. If they cannot be addressed, they become a POA&M entry with a certain risk level, which may not be acceptable to the AO.

M.1.6 Risk Management Framework Step 5: Authorize Information System

Task 5-1. Plan of Action and Milestones: Prepare the RMF plan of action and milestones (POA&M) based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

Preparation of the POA&M is not much different, if at all, for PIT systems, as compared to information systems. Following is an extract from the template for the security authorization package, which includes the POA&M.

DoD Plan of Action and Milestone (POA&M)					
(1) Date Initiated:		(6) System Type:		(10) OMB Project ID:	
(2) Date Last Updated:		(7) AO Name:		(11) Security Costs:	
(3) DoD Component:		(8) AO Phone:			
(4) System/Project Name:		(9) AO E-Mail:			
(5) System Identification:					

(1) Security Control Number (NC/NA controls only)		(3) Vulnerability Summary	
(2) Assessment Procedure			
(4) Vulnerability Severity Value			
(5) Risk Level			
(6) Source Identifying Vulnerability			
(7) Office/ Organization		(13) Weakness Comments	
(8) Resources Required			
(9) Scheduled Completion Date			
(12) Status			
	(10) Milestone with Completion Date		
	(11) Milestone Changes		

Figure 19. DoD Plan of Action and Milestone

It is important to note that for PIT systems during the design and development of the system, it may be prudent to draft the POA&M as soon as it is known that certain security controls cannot be implemented, cannot be implemented as expected (as for typical information systems), or are found to be non-compliant in early and often assessments, such that the design or implementation can be changed early and the programmatic impacts to cost, schedule, and performance can be minimized. The product baseline should be flexible for as long as possible prior to implementation so the design can be assessed against the current cyber threat.

Assuming tight resource constraints or huge programmatic impacts, it is advisable to prioritize entries in the POA&M based on the cybersecurity risk levels. That is, place up top/front the most impactful or the most risky entries, in order to draw the attention of the AO, who may be able to persuade those with funds to allocate them to cybersecurity fixes.

Also important is the need to clearly indicate what has been done to mitigate non-compliant security controls and what could be done to further reduce the risk, with a clear indication of the programmatic impacts, such that the AO understands what impact any authorization decision may have to the program and to the mission. Again, because PIT systems are unique and the IT is very closely tied to the functionality of the system and, therefore, mission success, the POA&M is a key element in communications with the AO for appropriate and timely decisions.

Adjusting the “session” example above, let’s assume the residual risk of not implementing the control was Moderate, which implies the weakness must be fixed at some point. If the POA&M reflects that it is possible and affordable to implement the control as planned, but it cannot be done until the next major release for the ground control component of the UABS (which is scheduled for 6 months from now), and that funds have been requested and are likely to be

approved in 2 months, the AO may be inclined to issue an Authorization to Operate with conditions, the conditions being that the control is implemented as specified in the POA&M. Conversely, if the POA&M simply states that the control is non-compliant and no fix actions are detailed, the AO is likely far less inclined to issue an Authorization to Operate, with or without conditions. Again, communicating to the AO via the POA&M what has been done, is being done, can be done, and will be done may be key. The POA&M is the program manager's key communication means to the AO.

Task 5-2. Security Authorization Package: Assemble the security authorization package and submit the package to the AO for adjudication.

The security authorization package is essentially the same for PIT systems as it is for information systems. The key is, however, to be sure each artifact (Security Plan, Security Assessment Report, Risk Assessment Report, and POA&M) clearly conveys the uniqueness of the system, any uniquely implemented security controls, any unique assessment of the controls, and the follow-on plans to fix weaknesses deemed uniquely relevant based on the impact to the mission.

Given how specialized the UABS example is, and assuming the AO is not familiar with the nuances of the system, it may be appropriate to include (or make available, possibly via eMASS) with the security authorization package any and all system artifacts (discussed above) for reference by the AO, should they have questions about the risk, assessments, implementation, or design decisions. Making these artifacts readily available can shorten the staffing time for packages and can convey due diligence on the part of the program office. No availability of artifacts can be misconstrued as those artifacts not having been prepared, when in reality due diligence was done and the artifacts were developed and are thorough.

Task 5-3. Risk Determination: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

This task is performed partly by the Security Control Assessor (possibly with some input from the program office) and partly by the AO. The more generic the Security Control Assessor is, the less likely they are to be able to know and understand the implications of certain aspects of the UABS (especially the bomber component), as to how they will impact mission operations. On the other hand, the presumption is that the AO was assigned due to their understanding of the mission and how any systems support that mission. If they are not completely familiar with the mission, in making risk determinations the AO should reach out to the mission owners for input on the risk determination, and the following risk acceptance decision. This is especially relevant in the UABS example. In fact, some DoD Components, particularly the Air Force in this example, have assigned specialized AOs (e.g., an Aircraft AO). In that construct, the Air Force also chose to assign specialized Security Control Assessors who are equally familiar with the aircraft systems and the cybersecurity implications; however, they may not be as familiar with the mission implications. Regardless, risk determinations are not made in a vacuum; program offices should be prepared to participate.

Task 5-4. Risk Acceptance: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

This is exclusively the role of the AO; however, as discussed above, they rely heavily on inputs from various sources. So again, the program office must be very clear in their communications to the AO, in particular in the POA&M.

M.1.7 Risk Management Framework Step 6: Monitor Security Controls

Task 6-1. System and Environment Changes: Determine the security impact of proposed or actual changes to the system and its environment of operation.

The system-level Information Security Continuous Monitoring Strategy was developed in Step 2 in anticipation of the need to monitor security controls over time. One of the components of that strategy must address intentional and unintentional changes to a system, and that is often executed by implementing several security controls in the configuration management family, such as:

- CM-3, Configuration Change Control
- CM-4, Security Impact Analysis

While the development/acquisition program office must have designed the system and procedures to allow such configuration management, much of the follow-on work here is performed by the sustainment program office, and the operational community for that matter, unless the acquisition PM is assigned lifecycle management responsibility.

Not all changes that could increase risk to the mission are related to configuration of the technical components of the system. In this UABS example, the bomber was designed to satisfy a certain capability need. Assumptions may have been made about the environment in which the bomber will fly (e.g., high altitude out of the range of enemy surface-to-air missiles), but those assumptions are not always valid over time. Enemy capabilities can increase, such as developing missiles with a greater range or higher ceiling of operation, or developing improved methods of cracking cryptographic algorithms used in the communication with the bomber to command and control it. The bomber (or the means of communicating with the bomber) may need to be redesigned for higher flight or redesigned with countermeasures to counter increased enemy capability. The implication is that the development/acquisition program office must consider design options (e.g., relatively autonomous components) that will allow the system to be cost-effectively upgraded to address new threats.

As to which changes may impact risk, the measuring stick is not “minor change” vs. “major change.” The bottom line is that ANY change to the system must be examined from a cybersecurity perspective to determine if the change weakens the cybersecurity posture, thereby creating new opportunities in cyberspace for the enemy to exploit the system. The rule of thumb is that if the change is to a component that implements a security control, a security control assessment must be performed on that component to determine the continued effectiveness of the control/s. But, other factors or interrelationships between components may drive the need to assess the entire system. Especially for highly specialized systems, such as this UABS example where proper functioning of the IT components are critical to the operation of the bomber (i.e., mission success), it is prudent to work closely with the Security Control Assessor to determine which proposed or actual changes may negatively impact the risk and, therefore, require an assessment and possibly a new authorization decision.

Task 6-2. Ongoing Security Control Assessments: Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

Selection of the subset of controls to be assessed over time is based on the criticality of the controls to the functioning of the system in question. That is, the more critical the function, the more frequently the controls supporting that function should be assessed. In this UABS example, the encryption of C2 links with the bomber are more critical than such things as whether or not the pilot has done the annual cybersecurity training or whether or not the maintenance crew inappropriately used remote access to update a software application on the bomber (while it was on the ground). But, we can see that these seemingly less important functions can, through a daisy chain effect, lead to more catastrophic failures. For example, if the remote access link was unknowingly compromised, an enemy could monitor the session, determine how/when changes are made, and either highjack the session or later pose as the authorized maintainer and upload software that provides unfettered access to and control of the bomber, at their time of choosing (e.g., when the United States chooses to bomb that enemy's assets).

This security control assessments should leverage the DOT&E cybersecurity assessments of system effectiveness and any existing vulnerabilities based on the current environment, including threat.

Therefore, we must fully understand how each security control supports the function of the system, examine the relationships between security controls, and determine how frequently each must be monitored. These relationships can be understood by examining the original traceability of security controls to system security requirements to implementation; we understand potentially how critical each control is to the system's functions and, therefore, to the mission.

Task 6-3. Ongoing Remediation Actions: Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.

This task is not much different from the actions taken by the program office to address non-compliant security controls found during the initial security control assessment, which are documented in the POA&M. However, because the system is in operation and the risk to the mission may not be acceptable, the program office may not have much time to resolve the weaknesses. The implication is that the sustainment program office must anticipate and program for the funds addressing any new weaknesses over the entire system lifecycle. In this UABS example, this aspect is critical; as it is likely the mission owner cannot tolerate the loss of such a capability.

The mission owner and the AO must strike a balance between the continued need for the capability (i.e., bomb selected targets) and the assurance to all stakeholders that the capability will not be lost or compromised due to cybersecurity weaknesses. The mission owner may be willing to continue operations at risk, but they may not fully understand or appreciate the risks. Those with cybersecurity responsibilities must be able to convey if/how enemies may exploit cybersecurity weaknesses and turn the bomber back on the mission owner or other friendly

entities. Seemingly benign or misunderstood cybersecurity weaknesses can have catastrophic effects for PIT systems.

Task 6-4. Key Updates: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

These documents are crucial in capturing and communicating to all concerned the cybersecurity posture of the system (i.e., risk) and what can be done, is being done, or will be done to correct any discrepancies and reduce the risk to an acceptable level. If these documents do not reflect reality over time, all stakeholders are left with a false sense of security and make inappropriate decisions, such as to continue operation of a UABS that has been compromised (e.g., by an advanced persistent threat actor) and can at any time be turned against friendly forces.

Task 6-5. Security Status Reporting: Report the security status of the system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.

DOT&E annually reports cybersecurity assessments of system effectiveness and any existing vulnerabilities based on the current environment, including threat.

As with the previous tasks, failure to report the security status will over time lead to undesirable consequences, up to and including bombing of friendly forces. All stakeholders simply must have current and correct information about the cybersecurity posture of the system to make informed decisions about the use of the system. They must have assurance the UABS has not been compromised, will not be compromised (to a certain degree of certainty), and will continue to perform its function in support of whatever mission it supports. Again, due to the integration of the IT into the basic function of the system and the potential for automated decisions, security status reporting is more critical for PIT systems than for typical information systems, where there is “wetware” (human brains) between the hardware/software and the execution of some mission.

Task 6-6. Ongoing Risk Determination and Acceptance: Review the reported security status of the system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.

This task is performed exclusively by an AO; but again, others (e.g., the program office) must clearly convey, in a timely manner, the information used to make these decisions. The more critical the IT is to the function of the system and the mission (e.g., this UABS example), the more the other stakeholders are involved in providing information to the decision makers.

In this UABS example, the mission owner may fully understand and appreciate that the enemy may have procured the ability to crack the crypto algorithms used to protect only the air tasking order. In other words, the enemy may know the bomber is coming to destroy them. However, the mission owner may be able to convince the AO not to rescind the Authorization to Operate, because it can be shown that knowing the bomber is coming simply reduces the likelihood that the enemy target will still be there when the bomber shows up. That is, the effectiveness of the

bomber is reduced, not eliminated completely. Note that the effective life of the air tasking order is very short, as compared to other information types. The mission owner may be willing to tolerate a degradation of capability, at least for a short time until the encryption algorithms protecting that information can be improved such that the enemy cannot crack them.

Task 6-7. Information System Removal and Decommissioning: Implement a system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

In this UABS example, it may be very straightforward and simple to decommission the bomber, but not necessarily the supporting ground systems, if those ground systems are highly interconnected and are being relied upon for inherited security controls. However, caution must be taken to, for example, remove and/or sanitize all sensitive or classified information or equipment (e.g., crypto algorithms/devices or all IT components) from the bomber before it is sent to the aircraft boneyard in the Southwest or to a museum.

For ground systems providing common controls to other unmanned aircraft or other ground-based systems, much coordination is required to gracefully terminate any service level agreements. Imagine how catastrophic it could be if the audit reduction and analysis function being performed by the system you are decommissioning was terminated, unbeknownst to other aircraft system or mission owners. Low and slow attacks (previously identified through audit reduction and analysis) could go unnoticed over time, the aircraft could be compromised, and the weapons of mass destruction could be turned against friendly forces at the enemy's time of choosing.

M.2 Example 2 – Practical Automobile Example

This is a notional example to illustrate how to incorporate cybersecurity into a program from the requirements stage through deployment.

M.2.1 The Requirement

Assume you have a requirement to get from your house to the mall and back, a distance of about 20 miles round trip. You need to get there safely, quickly, hopefully without getting too cold/hot or wet, while minimizing expense. You need to do this on a regular basis, and your decision must remain in place for several years.

M.2.2 Material Solution Analysis Phase

To decide the best way to accomplish this task, you come up with 3 alternatives – using a bicycle, a motorcycle, and a car. Among your evaluation criteria are speed, payload capacity, expense, availability, resistance to persistent threats (i.e., things that can prevent you from getting to the mall safely and quickly), and resilience when threats become issues (e.g. use of countermeasures or existence of a fallback plan). For the purposes of this example, we will focus on the resistance to threats by means of a metric. As part of your AoA team, you have a Red Team (a friendly force acting as an aggressor to maximize resiliency) doing a tabletop/brainstorming session about things that could stop you getting safely to the mall. Some ideas they come up with are a traffic accident, flat tire, weather, theft, traffic lights, getting lost, getting locked out, or engine break down.

VULNERABILITY/IMPACT ANALYSIS – FOR EACH ALTERNATIVE: During this analysis you quickly conclude that the bicycle has some pretty serious impacts that extend beyond your risk tolerance, because in a traffic accident you could die or be seriously injured, flat tire or theft will leave you walking, bad weather could be hazardous, and it will take a long time and your engine is likely to break down (i.e., a 20 mile bike ride is tiring). The motorcycle is better, but it is vulnerable in a traffic accident and in bad weather. The car better addresses those concerns (you are better protected in an accident), but you have some different risks like getting locked out. But, overall the car looks pretty good in the case of impacts compared to the other options (particularly when accounting for other measures of effectiveness such as speed and payload).

THREAT ASSESSMENT: Now that you have identified some potential impacts if those threats come to pass, you must figure out the likelihood of those impacts occurring. It turns out you have a really sneaky Red Team, and they think they could use cyber attacks to cause you to get into a traffic accident, cause a flat tire, aid in theft, cause you to get lost easier, lock you out of your car, or cause your engine to break down. Just taking the case of the car, they identify these potential attack vectors, however improbable.[62]

---

[62] Car and Driver has an interesting story on hacking:
http://www.caranddriver.com/features/can-your-car-be-hacked-feature

- Traffic accident or car break down: Modern cars use computer chips in many components, including the brake system and engine throttle. An adversary could conceivably "hack" your car, gain control of the throttle and brakes, and cause you to get into an accident. To cause the car to break down, a cyber attack can be used to disable the engine, such as kill the throttle, flood the engine, etc.
- Cause a flat tire: Some cars today have tire pressure monitoring systems that people depend on to tell them when tire pressure is getting low, and this is typically tied into the dashboard electronics, perhaps with a Bluetooth or Wi-Fi connection to actual pressure gauges on the tires. Over time, or in combination with a person physically increasing or decreasing the tire pressure, you may not get indications of over or under pressure until it is too late, resulting in a flat tire or a blowout.
- Theft: Most new cars today use remote keyless entry, and some have touch keypads in case you lock your keys in the car. Criminals can intercept the signal from your key fob and may be able to replay it when you're not there to gain access to your car. In addition, through cyber social engineering attacks, there are ways to get duplicate keys or a digital signature associated with a certain key to enable "hot wiring" even cars with special chips in the key required for ignition.
- Lock you out of your car: Same trick for theft, but as an added step, once they gain access to your car it is conceivable they could change the key access code. If you still have an actual key and the car still has mechanical locks, changing the code would not prevent you from entering, but there are some cars that no longer have physical keys – they depend entirely on the wireless key fob to gain entry.
- Cause you to get lost: You may be dependent on an in-dash GPS for navigating around town, which sometimes have a data port (such as a USB port) that allows you to upload new maps, software uploads, etc. Some cars may have Bluetooth or Wi-Fi capability that allows the car to access the internet to download new maps and update software – this is another potential attack vector. If an adversary can gain access to your dashboard electronics, they may be able to insert a virus into your GPS system to either stop it from working entirely, or worse, direct you to the wrong location or the wrong way down a one-way street.

ASSESS LIKELIHOOD OF OCCURRENCE: Note that identification of potential threats does NOT depend entirely on formal intelligence information. The Red Team came up with these based on their knowledge of the trade space of potential car concepts – depending on the specific type of car chosen, the threats may be more or less likely to occur. Intelligence information can help you determine the likelihood a threat is present (i.e., what is the capability, intent, and targeting of a given threat source, especially an adversarial threat source). For example, you may get intelligence information that there have been a lot of car thefts recently in the mall parking lot using key fob scanners bought off the internet, but those thieves appear to be unsophisticated and unlikely to be able to affect your engine control system. On the other hand, you might have intelligence information that a disgruntled computer programmer coworker that you just beat out

for a promotion is in the neighborhood – so there may be an elevated likelihood of someone tampering with your engine near your home.

Taking the potential attack vectors, impacts, and likelihood of attack into account, you can develop an initial matrix for cyber risks to your "mission", and formulate it into a risk cube. At this point, you still have not chosen a specific design, but you have a notional idea of the greatest cyber risks to your chosen concept. Only after you chosen a specific design, and identified specific vulnerabilities associated with your design, can you get a realistic full cyber risk assessment. As a result, we will refine this risk assessment in the technology maturation and risk reduction phase and engineering and manufacturing development phases.

SELECT INITIAL SECURITY CONTROLS: Assume that for now, despite the known cyber threat assessment for the car, when weighted against resistance to cyber threats as a whole and all of the other measures of effectiveness (MOEs), you choose the car as your best option to develop. You might also have ideas of cybersecurity controls [preventive measures or countermeasures] you can add to a car. Because they can be costly, you try to select those that are most likely to help make your trip to the mall (your mission) more resistant to cyber attack, or able to restore operability during an attack. So we will move onto the technology maturation and risk reduction phase. You develop a test strategy that says you will want to do a Blue Team assessment on your concept(s) in the technology maturation & risk assessment phase, and some further Blue Team (simply put, Blue Team defends the network for a limited duration) testing of your refined design during developmental test and evaluation (DT&E). Lastly, you recognize that a cyber attack should be part of a full Red Team assessment, not in OT&E where you want to measure performance against most of the MOEs/measures of performance (MOPs). You plan to test your resistance to countermeasures (both physical and cyber) in a contested cyber threat environment during a Red Team assessment.

M.2.3 Technology Maturation and Risk Reduction Phase

IMPLEMENT SECURITY CONTROLS IN PROTOTYPE PHASE: Now that you know the threats in the technology maturation & risk reduction phase, you want to see what you can do to minimize the risk. Thus, part of your technology development strategy is to prototype two different car design concepts in an attempt to further quantify and buy down the risk. The first design concept you choose to protect against the cyber threat is to go old school – you are going to build a car that has no GPS, has mechanical door locks, uses rack and pinion steering, hydraulic brakes with no anti-lock, and a carburetor-based engine design. Such an austere design essentially takes you offline—it is like operating without the performance benefits of being net-centric—but it protects you from these cyber threats. For the second design concept, you choose a modern car design with fuel injection, anti-lock brakes, 4-wheel steering, in-dash GPS, digital entertainment console, in-dash maintenance console, electronic locks and windows, but with the top of the line security features (key with digital chip, electronic ignition disable etc. Before you get too enamored by all the high-tech toys, be sure the technology is really needed and can be secured adequately).

After you construct your two prototypes, you bring in a blue team to assess your vulnerabilities. On the old-school design, they find that you are pretty resistant to the cyber threat – on the risk cube, all of the probabilities drop below the bottom row of the cube as there are no cyber dependencies. No cyber controls are required as you have no cyber vulnerabilities. However,

when you assess against some of your other requirements and non-cyber countermeasures, you realize it is far easier to steal or disable the car by mechanical means – a hanger through the window to unlock the car, hot wire the car, or pulling the distributor plug from under the hood to disable the car. In contrast, your Blue Team assesses that while there are some potential cyber vulnerabilities to the modern car, the modern security features disable all of the mechanical means of countering your mission, and even the cyber means are not trivial to do so. Furthermore, they are able to identify a few controls that you may be able to implement to further reduce the likelihood of cyber attacks being successful. The first control is to simply disable the Wi-Fi and Bluetooth connectivity on the in-dash GPS and entertainment console. The second control is to look around your car before you unlock it to see if there might be anyone nearby looking suspicious with some piece of electronic equipment you do not recognize and, if so, use the key instead of the keyless entry. The third control you identify is simply to keep the car locked at all times – with Wi-Fi disabled, access to the in-dash electronics and the engines under the hood are far more limited. However, an adversary could still break a window or open the latch on the hood to gain access to cause or initiate cyber damage. Implementation of these simple controls greatly mitigates your cyber risk, but the controls do not mitigate the risk entirely.

Bottom line, despite the identified vulnerabilities, you feel the pros of the modern car outweigh the cons with respect to the carburetor-based car, and you down-select to that prototype based on the outcome of the prototype demonstration and Blue Team assessment.

REFINE SECURITY CONTROLS: As a result of the assessment, you modify your requirements for the car and proceed to the Preliminary Design Review (PDR) stage in an attempt to mitigate the threat. Specifically, by the PDR, you decide the threat to the engine has the greatest potential consequence, so you decide there needs to be an anti-tamper system added to the engine, but it will not be fully designed until the Engineering and Manufacturing Development (EMD) phase. You complete the Test and Evaluation Master Plan (TEMP), where you lay out specifics on the types of tests you want to perform for both the Blue and Red Team testing, now that you know you want to operate a modern car design. The TEMP in this case will cover specific attempts to mess with the car engine, mess with the in-dash electronics, and gain access to your car, but it will not test for means to give you a flat tire or lock you out of your car, as your Blue Team assessment during this test phase assessed the likelihood of both of those attack vectors as extremely low. You then draft the Acquisition Strategy and request for proposal (RFP), and take it to your Chief Executive Officer (CEO) for approval to develop the car, and assuming approval, release the RFP. Once you get your bids back, you award the EMD contract at Milestone B (MS B).

M.2.4 Engineering and Manufacturing Development Phase

IMPLEMENT SECURITY CONTROLS: During the EMD phase, your team assesses that some minor additional mitigations to the in-dash electronics are required, while we still need to fully design the anti-tamper system for the engine block. For the in-dash electronics, with the Wi-Fi and Bluetooth disabled (controls identified during TMRR phase), the only remaining entry point into in-dash electronics is the USB port. You cannot disable the USB port, because you do need some mechanism for upgrading the maps and GPS software, as well as allowing maintenance technicians to access some information from the dash. Saying that, you can make it far more

difficult to hack if you add specific user accounts and password protect those accounts, or even add a biometric identification system (fingerprint reader) as an added protection. In this case, a thief or saboteur could still theoretically gain access to the systems, if they somehow manage to get all the proper credentials; but, you've made it harder by adding two layers of authentication, as well as requiring direct physical access.

This is for someone who understands the engine block design.

> On the engine block design front, your engineering team delves into the design. At the simplest level, the way it works is that individual chips scan the bus for a message that matches their identification (ID), and then grab and process the data packet. An analogy is your teacher has a stack of graded exams on the desk, so you walk up, scan each exam for your name, and when you find the one with your name on it, you pick it up and take a look at it (and ostensibly take some action based on what you see). Looking at it from another perspective, at PDR they had designed the electronic engine controls to use standard commercial-off-the-shelf (COTS) chips that operate on the Control Area Network (CAN) bus. A standard CAN bus message is a 94-bit packet transmission consisting of an 11-bit identifier, some control bits, an error checking field, and up to 64 bits for data.

In an ideal world, the car engineers designed each chip to know the IDs of other chips they need to talk to, know the range of data or commands each chip will accept, and send messages to other chips compliant with that protocol. The problem under this approach is that all of the chips on the CAN bus trust each other to "do the right thing," so they do not verify the message came from the source they think it did (authentication), and they typically do not check that the data it sends is valid (integrity). (Lack of confidentiality is probably something you would not need to worry about in this scenario, as we are only concerned with attackers causing adverse effects, not that anyone can see the traffic).

This is really for someone who understands data protocols and encryption, so skip this section if that is not your cup of tea.

> So this is what your team chooses to modify. They decide to use the extended version of the CAN protocol instead of the basic protocol, which adds an additional 29 bit identifier after the 11 bit identifier. They encode the ID of the source chip in the additional 29 bits. They encrypt everything except the identifiers with the private key of the source. Then, it sends the message.
>
> When the destination chip sees its identifier, it examines the ID of the source chip in the next 29 bits. Doing an internal table look up to find the public key associated with that device ID, it uses the public key of the source to decrypt the data/command, and does a cyclic redundancy check (CRC) on the error field. If the CRC passes, it has successfully authenticated the message. The last step is it internally validates the data command is in a valid range, and if it is, it processes the data and takes appropriate action.

> There are other alternative approaches to doing this such as using a symmetric encryption key. However, this is theoretically more secure than symmetric key, because the symmetric key has to be shared amongst all chips for any of them to talk to one another. If an adversary gets access to one chip and is able to compromise it, he has the "keys to the kingdom" for that car – any bogus message he has that chip send will be trusted by every other device.

By taking this approach, we have eliminated a whole host of controls that might be required to mitigate an attack against the system. Specifically, we are no longer concerned about physical access to the engine block or even the possibility of planting a bogus chip on the bus – without both the public AND private encryption keys for the chips, they will be unable to take control of the engine, brakes, etc., even if they have physical access to the system. In addition, other additional control measures such as a host-based security system or bus scanner would not be required as well.

After you successfully implement the design and are getting ready for Milestone C (MS C), you need to do the final developmental test. You do your standard testing on the system as well as the Blue Team testing.

But, uh-oh! Although the Blue Team verifies you've eliminated the vulnerability in the engine, and dramatically reduced the risk of access to the in-dash electronics, you discover your cyber fixes have degraded the performance of the engine to the point that the engine timing is off; the brakes are sluggish, etc. – not an acceptable outcome.

Unfortunately, this is not an easy fix. Costly solutions are implemented when consideration for cybersecurity is not done from the very start.

> Your fishbone analysis has determined root cause that the reason this was slow is that public key encryption generally requires much longer keys, and thus much longer times to encrypt and decrypt, than symmetric keys for the same level of security. In other words, the performance hit due to your cyber controls was unacceptable from a mission performance standpoint. You could go back to the original CAN bus design with no encryption and look at imposing additional physical access controls and/or host-based security system and/or bus scanner. Or you could pursue an alternative design such as going to a symmetric key system.
>
> In a symmetric key approach, every chip on the bus would be loaded with the same encryption key. Each chip would encrypt the CAN message with the symmetric key, and the destination chip would decrypt it with the same key. Authentication is achieved in the same way as Public Key Infrastructure (PKI) – if we pass the CRC check, we are authenticated. This has the added advantage of less read-only memory overhead to store all of the public keys – only the symmetric key needs to be stored, and no table lookup is required to find the key in the decryption process.

Your engineering team assesses that the symmetric algorithms should be fast enough to eliminate the latency that plagued the PKI-based approach, and should be cheaper to retrofit than

implementing the other controls as only the encryption algorithms have to be changed, not the authentication and data validation steps. Also, the other controls are expected to cause overhead/latency within the engine and may be no better than the PKI approach. So, you implement it and repeat DT&E.

This time, the system performance is at an acceptable level, and the Blue Team verifies this does stop most cyber attacks. For completeness, though, you give them access to the hood of the car and let them remove one of the chips. They take it back to their lab and recover the symmetric key, create a new bogus chip with the symmetric key in it, and reinsert it back into the car. Once they do this, they demonstrate that they can take control of the car.

But that's OK. In your risk assessment, you show the probability of actually being able to do what the Blue Team did as requiring a sequence of miracles – gaining access to a locked car, getting the chip back to the lab, finding the encryption key, creating a duplicate bogus chip with the symmetric key embedded, and reinstalling the chip back in your car, all within a time duration that you would not notice someone had broken into your car and modified the car (assuming the car would not work without the removed chip). This is well in the "green" risk category according to your assessment, and you are willing to accept the remaining risk. Therefore, your Program Executive Officer (PEO) certified you are ready for operational test and evaluation (OT&E), and you proceed to MS C for Milestone Decision Authority (MDA) approval to proceed into OT&E.

M.2.5 Production and Deployment

You go through your test with the typical operators to verify operational performance. You get through OT with a few deficiencies, such as the car did not accelerate fast enough, you almost hit a pedestrian at the intersection, and the GPS maps were not updated, but overall it went pretty well.

Now they bring in an aggressive Red Team. You discover your operators forgot to lock the door one day at the mall, and the Red Team gained access to the car. On that day, they tried to upload a virus into your car's GPS unit using the USB connector, but they were thwarted when they got to the password protection. They could have eventually broken the password, but not before you returned from the mall. Then the next day, they went old school and broke the passenger window with a crow bar. They popped the hood, brought out their laptop with a CAN diagnostic table attached to their serial port, and tried to send some bogus commands to the CAN bus. However, as the chips in the system only recognize encrypted data and commands, that did not work. Then, they swapped out your oxygen sensor chip with an off-the-shelf variant that was loaded with malicious code to send commands to peg the accelerator to the floor, and left before you returned. When you returned, you noted the smashed window with dismay, but you started up the car and drove home without too much of an incident, although you noticed your acceleration seemed a bit off.

Noticing this, you take the car to the maintainer to check it out. When the maintainer (who also has the symmetric key to enable diagnostics) tries to figure out what's wrong, he notices that he cannot talk to the oxygen sensor at all. When he pulls it out to take a look at it, he discovers that it is a bogus chip. Red Team is busted! He replaces the chip with one with the proper encryption key.

But the Red Team is not done yet. The window is not fixed yet, so they replace a different chip. Realizing they could not take control of the car, they go for a denial of service approach. Their new bogus chip simply sends a stream of garbage commands over the bus, flooding the bus so none of the chips are able to talk to each other. Neither the Intelligence Community nor your early Red Team members anticipated this threat early in the program, so you never developed a control to protect against it. Too bad! Say the operational testers, "We got you!" They declare your system not operationally effective, because it could not be operated within that threat environment, and they write that up in your report.

Does that mean you have to go to the start again and redesign your system to account for the evolved threat? Not necessarily. Your team goes through what the Red Team did and assesses how likely that scenario actually is in the real world, and what the impact is. As you perform your analysis, you quantify the series of miracles that has to occur for the adversary to be able to perform the attack the Red Team eventually got away with, and you show that while the attack is possible, it is extremely low likelihood. Furthermore, you also assess that the impact of the denial of service attack (i.e., the car does not work or reactions are very slow) is far less serious than if they were actually able to take control of the accelerator and actually disable the brakes while flooring the accelerator, etc.

Now you bring in the operational user and make your case to them. They agree the risk of that particular mode of attack is at the acceptable level (i.e., it is within their risk tolerance), although they levy a high risk deficiency report (DR) on the program to add additional controls during sustainment or, if not possible, at the next block upgrade. Furthermore, they say that even if there is a remote possibility the car will not work properly in that situation, the rest of the time they do not have to walk 10 miles to the mall, in the snow, uphill both ways, because they have this great car to take them there now.

You bring the user with you to the full rate production decision meeting with your MDA. DOT&E brings up the weakness they observed, and the user states that they agree that the vulnerability exists, but they can live with it, and they love the living daylights out of the car, even with this pathological failure case. You also chime in and point out that you are still carrying this vulnerability as a DR that you will fix as funds become available. The MDA hears all the arguments, thanks all parties for their inputs, and gives the go ahead to start full rate production and deployment, with a note in the acquisition decision memorandum to fix the vulnerability as funds become available.

Congratulations! You have successfully implemented robust cyber protection in your system from concept development through deployment of the car with a minimal amount of externally imposed controls (and associated costs), and it is inherently more secure than even if all of the other controls were implemented without your cyber-resistant design, through the use of a risk-based approach to cyber protection.