DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

SYSTEMS SECURITY ENGINEERING CYBER GUIDEBOOK

Version 4.0

26 July 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Secretary of the Air Force, Public Affairs (SAF/PA) Case #: 2021-0424. Requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

ENDORSEMENTS

The need for this guidebook and its contents has been endorsed by the following organizations:

- **United States Air Force Life Cycle Management Center**
- **United States Air Force Space and Missile Systems Center**
- **United States Air Force Nuclear Weapons Center**
- **United States Air Force Rapid Capabilities Office**
- **Naval Air Systems Command (NAVAIR) Cyber Warfare Department**
- **National Defense Industrial Association (NDIA) Systems Security Engineering Committee**

Table of Contents

Table of Tables

Table of Figures

EXECUTIVE SUMMARY

This Government Accounting Office (GAO)[1] highly lauded Department of the Air Force (USAF) Systems Security Engineering Cyber Guidebook (SSECG) implements Cybersecurity and Cyber Resiliency policies and standards for all USAF Space and Weapon Systems, their Mission Essential and Supporting Systems, and Defense Business Systems (DBS). Space and Weapon Systems are assumed to be Cyber-Physical Systems (CPS) hereafter. The SSECG provides a single source for guidance on Systems Security Engineering (SSE) within the USAF space and weapons system acquisition community. It is intended to assist Program Offices in performing the System Engineering (SE) and System Security Engineering (SSE) analyses needed to understand the Cyber Engineering aspects of their Space and Weapon Systems, and Defense Business Systems. It encompasses a holistic look at different aspects of SSE (e.g., Cybersecurity, Trusted Systems and Networks, Anti-Tamper, Information Protection and Cyber Resiliency), and outlines a single workflow process to integrate Program Protection (PP) and SSE activities into traditional SE processes – with the goal of helping program offices in designing and verifying that Space and Weapon Systems and DBS that are more Cyber Resilient and Cyber Survivable, not just Cyber Secure.

The SSECG workflow processes provided in this document distills all the requirements from applicable policies and standards to support consistent contract language executable through the Adaptive Acquisition Framework (AAF) life cycles. Additionally, the SSECG workflow processes account for the Risk Management Framework (RMF) requirements, as well as, Cyber Test and Evaluation (T&E) requirements and test phase activities (specifically those of the Mission Based Cyber Risk Assessment [MBCRA]). A description of the relationships to RMF and T&E is located in Appendix F.

In the Department of Defense (DoD), a Weapon System is defined as a combination of elements that function together to produce the capabilities required for fulfilling a mission need. These elements include hardware and software, and their associated adapters and interfaces. Modern Weapon Systems are CPS with embedded intelligence that include engineered interacting networks of physical and computational components. DoD Space Systems are defined as a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service. A Space System typically has three segments: a Ground Control Network, a Space Vehicle, and a User or mission network as an Actor. These systems include Government national security space systems, Government civil space systems, and private commercial space systems.

This SSECG was developed to:

- Meet the recently promulgated DoD requirements and processes delineated in the System Engineering for Defense Systems and Mission Engineering Guide.
- Provide a common starting point for Acquisition Category (ACAT) and National Defense Authorization Act (NDAA) for Fiscal year 2016, Section 804 programs to ensure SSE is an integral aspect of Program Management and SE, and that the required AAF acquisition-related documents and artifacts are developed to support their notional and required approval timelines. The SSECG

[1] “GAO-21-179, “Weapon Systems Cybersecurity - Guidance Would Help DOD Programs Better Communicate Requirements to Contractors”, p. 26, March 2021

facilitates the development of well-defined, complete plans and schedules for use in a program's execution, thereby reducing system and program vulnerability risks that will increase the probability of the program's success.

- Provide guidance for compliance with Director of National Intelligence (DNI), CNSSI 1253[2] standards for National Security Systems (NSS) (e.g., Space and Weapon Systems).

- Provide the standards for modeling Space Systems and Weapon Systems as CPS.

- Provide a consistent approach and processes for developing Space and Weapon Systems that apply SE principles in a standardized, repeatable, and efficient manner that aids in identifying security vulnerabilities, requirements, and verifications that minimize mission and safety critical risks. Also included is guidance on SSE Workflow Process applications that can provide detailed, comprehensive Cybersecurity and Cyber Resiliency requirements for Space and Weapon Systems.

- Improve USAF-critical, enterprise-wide Space and Weapon System risk assessment and management activities to facilitate a more effective, efficient, and cost-effective SSE execution.

- Integrate Cybersecurity and Cyber Resiliency for Cyber Survivability concepts early in the Adaptive Acquisition Framework (AAF) process.

- Promote the development by vendors of trustworthy, secure computer systems, software, and Space and Weapon Systems aligned with DoD and USAF processes, requirements, and guidance.

- Integrate Supply Chain Risk Management (SCRM) guidance and procedures into SSE to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout a Space and Weapon System's AAF life cycle. The transition from design to manufacturing data and drawings, the resultant Manufacturing Bill-0f-Materials (BOM), Non-Conformal Material, and the effects of the manufacturing processes on SSE are introduced as a part of SCRM risks.

- Allow tailoring to each program's or project's specific Critical Operational Issues (COI) needs.

The SSECG guidance should be tailored and scaled according to the size and of the program. All SECG reference documents are included in the Appendices.

[2] CNSSI 1253, "Security Categorization and Control Selection for National Security Systems", 27 Mar 2014

FOREWARD

SSECG Version 4.0 reinforces the direction delineated by the E.O., “Improving the Nation’s Cybersecurity” of 12 May 2021. It introduces the recent Department of Defense (DoD) policy changes to include Mission System Engineering, System Engineering for Defense Systems, Cyber Physical Systems (CPS), and Space Systems Cybersecurity principles and traffic management policies for cyber survivability that are harmonized with the SSECG existing Functional Thread Analysis (FTA) workflow process.

This SSECG Version 4.0 supersedes the previous SSECG Version 3.0.1 formally issued on 29 January 2021 and the Program Protection (PP)/System Security Engineering (SSE) Guidebook, Version 2.0 formally issued on 12 March 2020.

To effectively execute the activities of this SSECG, it is recommended that the User have at least a Defense Acquisition University (DAU) Level 2 certification in the required functional area (e.g., engineering, program management, etc.) or similar practical experience in Space and Weapon Systems acquisition programs.

DAU certification standards and required acquisition courses are listed here:

https://icatalog.dau.edu/onlinecatalog/CareerLvl.aspx

Comments, suggestions, or questions on this document should be submitted using:

USAF SSE Cyber Guidebook Comments Resolution Matrix (CRM)

and emailed to the Cyber Resiliency Office for Weapon Systems, Acquisition Support Team, System Security Engineering Lead, Ms. Katie Whatmore, NH-04 USAF AFMC AFLCMC/EN-EZ/CROWS at:

katie.whatmore@us.af.mil

The SSECG CRM, a Microsoft Excel-based form, embedded in Appendix J, is used to collate USAF and DoD comments for the SSECG compliance with current directives and standards, and to meet the immediate needs of the Program Offices developing and sustaining the Space and Weapon Systems, legacy, modern and those still in conceptual design.

APPENDICES SUMMARY

APPENDIX A - SSE Acquisition Guidebook

Guidance for incorporating SSE into programmatic documents as well as guidance for including SSE into Requests for Proposals (including tailorable requirements language). It is referenced for additional guidance throughout the main document. It will continue to be updated and released as part of this SSECG.

APPENDIX B – Guide for CPI/CC Identification

Includes a process and guidance for identifying Critical Program Information (CPI) and Critical Components (CC). It is referenced for additional guidance on various topics in the main document. It will continue to be updated and released as part of this SSECG.

APPENDIX C – Functional Thread Analysis

How to perform a system functional decomposition to identify mission and safety critical functions.

APPENDIX D – Attack Path Analysis

Information on how to identify potential cyber-attack paths within a system.

APPENDIX E – SSE Requirements Implementation Assessment

A recommended, risk-based, periodic assessment during system development to verify how well the SSE requirements are being allocated against the system's critical functions.

APPENDIX F – Relationship to Other Processes

Mapping of the SSE Cyber Workflow Process to the DoDI 5000.02, Adaptive Acquisitive Framework (AAF) pathways, DoD Cyber Test & Evaluation, and the Risk Management Framework (RMF).

APPENDIX G – Definitions

APPENDIX H – Acronym List

APPENDIX I – References

APPENDIX J – Templates

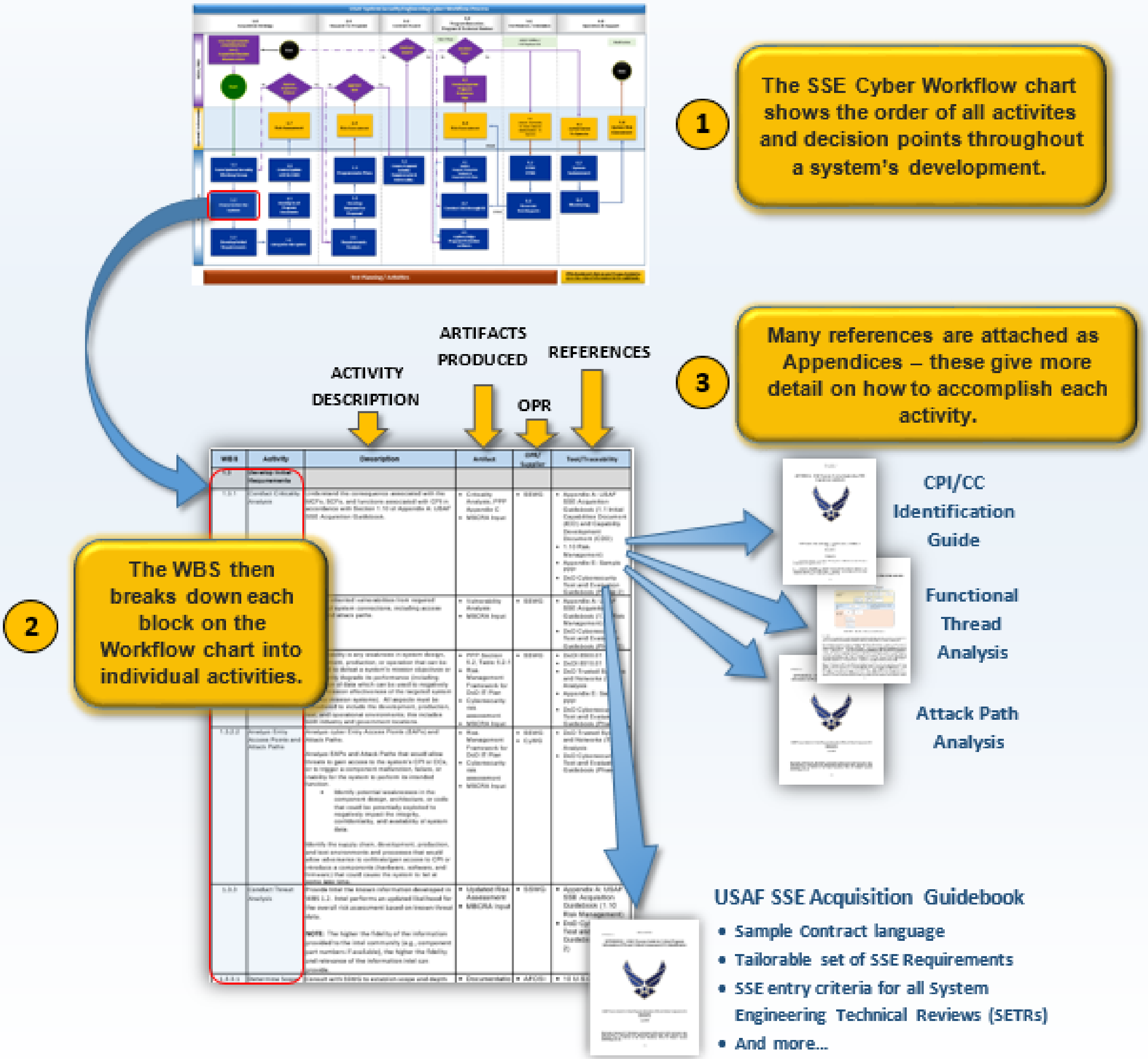
Includes the Guide's Comments Resolution Matrix (CRM) and the Attack Path Analysis (APA) templates.

RECORD OF CHANGES

Version	Effective	Summary
4.0	26 July 2021	• Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	• Addition of Space Systems relevant content. • Addition of WBS applicable space systems and task/sub-tasks. • Updated Appendix F • Updated references.
3.0.1	29 Jan 2021	Introduction of AAF, CPS and MRAP-C.
3.0	05 Nov 2020	• Changed the name of the previous USAF PP/SSE Guidebook to the USAF SSE Cyber Guidebook. • Revised: Figure A-2 Cyber Survivability Pyramid. • Added: DoD AAF lifecycle processes; Appendix J, USAF Cyber Guidebook's Comments Resolution Matrix (CRM), Excel workbook. • Revised: All SSE Cyber Workflow process charts to reflect the AAF and T&E WBS tasks. • Revised: All appendices in their order of presentation. • Deleted: Use Cases and Sample PPP from the USAF PP/SSE Guidebook (now used for training).
2.0	Mar 2020	• Added Executive Summary. Reformatted the document for consistency across appendices, and added appendices to include the App A: USAF SSE Acquisition Guidebook, USAF Combined Process Guide for CPI/CC Identification, App C is a detailed explanation on Functional Thread analysis, App D contains an aircraft use case for the overall SSE process, App E contains a sample PPP template, App F outlines a method for reviewing SSE requirements implementation, and App G shows a mapping of the PP/SSE Process to Risk Management Framework activities. • Included updates throughout from comments from the National Defense Industrial Association (NDIA) SSE Committee. Included several figures in Section 4 to help users link the PP/SSE Process to the Acquisition Life Cycle phases. Included many changes throughout the Work Breakdown Structure in Section 4 to better integrate and highlight cyber test and evaluation activities into the various process steps, including the Mission-Based Cyber Risk Assessment. Within the WBS, interchanged steps 1.3 and 1.4 so that the categorization is after the initial requirements are developed. • Changed the name of the document from a "Process Guidebook" to a "Guidebook" now that the combined document has more varied information within.
1.0	Jan 2019	Initial Release

How to use this Guidebook

The SSECG Guidebook's presentation order mirrors its USAF System Security Engineering Cyber Process Workflow chart. Each process is delineated by existing DoD, USAF & Government directives or standards. Each process is directly linked to its respective WBS Tasks or Sub-Tasks tied to their suggested contractual language.



1 The SSE Cyber Workflow chart shows the order of all activites and decision points throughout a system's development.

2 The WBS then breaks down each block on the Workflow chart into individual activities.

3 Many references are attached as Appendices – these give more detail on how to accomplish each activity.

USAF SSE Acquisition Guidebook

- Sample Contract language
- Tailorable set of SSE Requirements
- SSE entry criteria for all System Engineering Technical Reviews (SETRs)
- And more…

1.0. BACKGROUND.

The Task Force Cyber Secure Establishment memorandum, dated 20 March 2015 and signed by the Chief of Staff of the Air Force, stated, “The US Air Force’s ability to fly, fight, and win in air, space, and cyberspace is threatened by increasingly competent adversaries in the cyberspace domain.” As the world moves towards an era where cyber technology is thoroughly embedded into everything engineered, including weapons systems, the mission assurance posture driven by concerns in cyber technology needs to be consistent with those used in the air and space domains. This requires an evolution from an after-the-fact, compliance-centric perspective for acceptance, to an engineering-based system that is holistic and risk-informed for all engineering and acceptance activities. A methodical, collaborative approach is needed to leverage Systems Engineering (SE) and security best practices to meet the intent of existing policy, mandates, and key acquisition milestones. Figure 1 depicts the complexities of existing policy requirements that program offices must currently navigate to accomplish SSE.

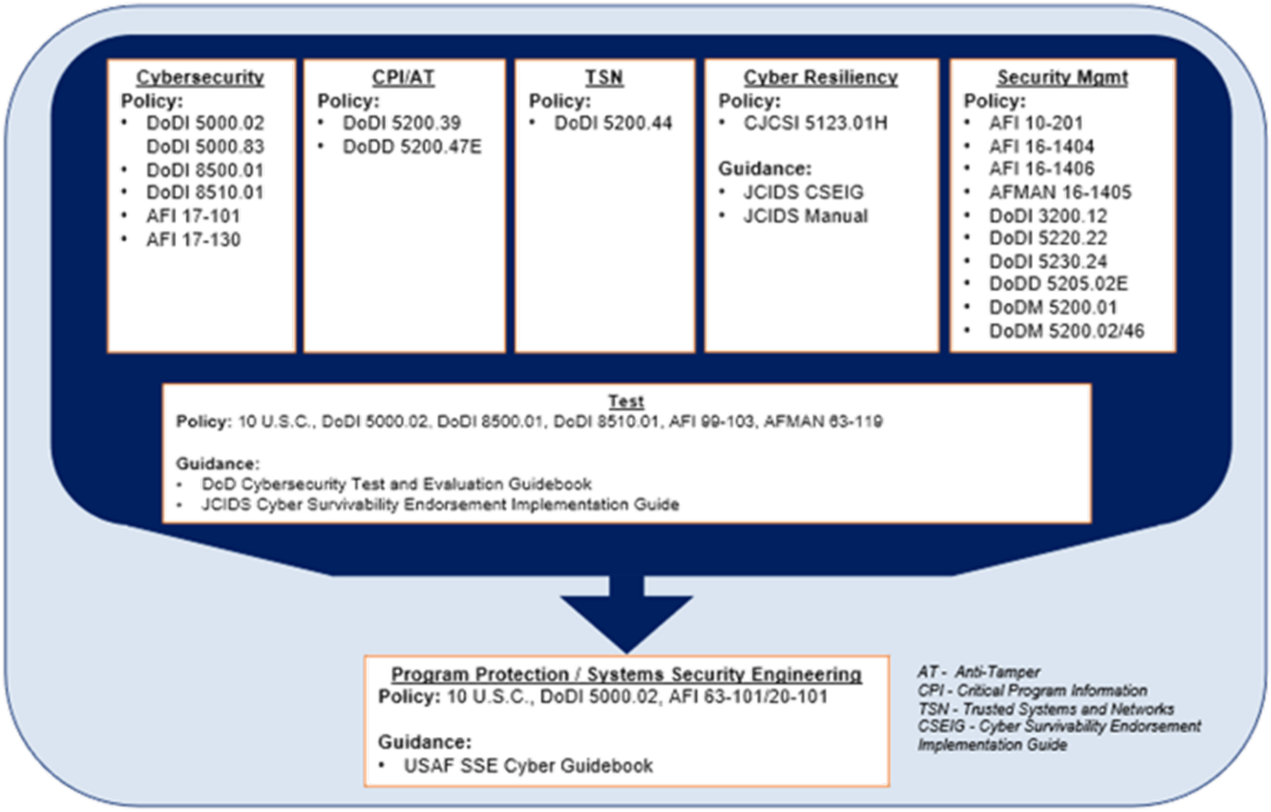

Cybersecurity
Policy:
• DoDI 5000.02
DoDI 5000.83
• DoDI 8500.01
• DoDI 8510.01
• AFI 17-101
• AFI 17-130
CPI/AT
Policy:
• DoDI 5200.39
• DoDD 5200.47E
TSN
Policy:
• DoDI 5200.44
Cyber Resiliency
Policy:
• CJCSI 5123.01H
Guidance:
• JCIDS CSEIG
• JCIDS Manual
Security Mgmt
Policy:
• AFI 10-201
• AFI 16-1404
• AFI 16-1406
• AFMAN 16-1405
• DoDI 3200.12
• DoDI 5220.22
• DoDI 5230.24
• DoDD 5205.02E
• DoDM 5200.01
• DoDM 5200.02/46
Test
Policy: 10 U.S.C., DoDI 5000.02, DoDI 8500.01, DoDI 8510.01, AFI 99-103, AFMAN 63-119
Guidance:
• DoD Cybersecurity Test and Evaluation Guidebook
• JCIDS Cyber Survivability Endorsement Implementation Guide
Program Protection / Systems Security Engineering
Policy: 10 U.S.C., DoDI 5000.02, AFI 63-101/20-101
Guidance:
• USAF SSE Cyber Guidebook
AT - Anti-Tamper
CPI - Critical Program Information
TSN - Trusted Systems and Networks
CSEIG - Cyber Survivability Endorsement Implementation Guide

Figure 1   SSECG Policies

1.1. DAF Systems Security Engineering Cyber Guidebook

Systems Security Engineering (SSE) is an element of Systems Engineering (SE) that applies scientific and engineering principles in a standardized, repeatable, and efficient manner to identify security vulnerabilities, requirements, and methods of verifications that minimize risks. SSE delivers systems that satisfy stakeholder security and resiliency needs for space and weapon system operations in today's cyber-contested environments. One method of doing this is by using SSE Workflow Processes to design systems in a way that makes them more resilient to cyber-attacks.

Cyber Resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber Resiliency is a key outcome of SSE to enable Space and Weapon systems, and their Mission Essential and Supporting systems to operate in cyber-contested and hostile natural environments in order to complete their missions.

A Space System is a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, the portion of space systems that operates in space that provides a space-based service.

A Weapon System is defined as a combination of elements that function together to produce the capabilities required for fulfilling a mission need. Elements include hardware, equipment, and software.

The SSECG is the starting point for the acquisition professional to understand the activities/tasks and timelines to execute Program Protection (PP) and SSE through the SE process for both of these military systems to include:

- Mission Engineering (ME)
- Systems Engineering for Defense Systems
- Technical Risk Assessments

Operational Resiliency, Mission Assurance, and Mission Engineering are considered distinct disciplines and concepts that must be addressed within the System Engineering for Space and Weapon Systems.

The SSECG enables Acquisition Category (ACAT) programs and National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, Section 804 programs to guarantee that SSE is an integral aspect of program management and SE. The process also ensures the required acquisition documents and artifacts are developed to support required SE technical reviews and milestones. This document provides guidance for all Air Force (AF) acquisition organizations, to include the AF Life Cycle Management Center (AFLCMC), AF Nuclear Weapons Center (AFNWC), and Space and Missile Systems Center (SMC). The guidance can also be tailored to fit the needs of other DoD acquisition organizations to include the Army, Navy, and Marine Corps.

The SSECG serves to integrate the processes for identifying vulnerabilities in system design, sabotage or subvert a Space and Weapon System Mission Critical Functions (MCF) or Critical Components (CC), and delivering affordable and effective capabilities through more streamlined acquisition and System Security Engineering (SSE) processes of: DoDI 5000.88, "Engineering of Defense Systems," DoDI 5000.02, "Operation of the Adaptive Acquisition Framework," DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," and DoDI 8500.01, CH-3, "Risk Management Framework (RMF) for DoD Information Technology (IT)," and DoD "Mission Engineering (ME)" Guidebook that address or delineate:

- Anti-Counterfeit Practices
- Anti-Tamper (AT)
- Cybersecurity
- Exportability Features
- Hardware Assurance (HwA)
- Procurement Strategies
- Secure System Design
- Security (Security Management/ Information Protection [IP])
- Software Assurance (SwA)
- Supply Chain Risk Management (SCRM) & Cyber-SCRM

The SSECG is to be used in conjunction with the USAF SSE Acquisition Guidebook (SSE AG), included in Appendix A. The SSE AG provides detailed comprehensive Cybersecurity and Cyber Resiliency requirements language for space and weapon systems.

This SSECG, along with Appendix A, provides the roadmap to navigate requirements in order to comply with policy and regulations and define the artifacts necessary to develop and support the **System Requirements Document (SRD) / System Specification** (to include test), **Statement of Objectives (SOO) / Statement of Work (SOW)**, **Contract Deliverable Requirements List (CDRLs)**, **Section L**, and **Section M** for the Request for Proposal (RFP). The principles and guidance provided in this document can be applied at any point through the life of a space and weapon system for "new start" programs, as well as, modification or modernization programs.

1.2. Program Protection Plan Coordination and Approval.

By executing the process in this SSECG, artifacts will be generated that will populate the Government owned Program Protection Plan (PPP) and be provided to industry during contract solicitation. The PPP is a living document and will be submitted for approval, in accordance with Major Capability Acquisition, Operation of Middle Tier Acquisition (MTA), Urgent Operational Needs (UON) and Software Acquisition (SA) at each acquisition pathway decision points. DoD guidance on minimal content is identified in:

- DoDI 5000.83, "Technology and Program Protection" for Program Protection Plan (PPP) para. 3.4.c p 21 and para. para. 3.4.c p 21 and para. 3.5 p 23. 20 July 2020
- AFPAM 63-113, "Program Protection Planning for Life Cycle Management", 17 October 2013
- AFI 63-101/20-101, "Integrated Life Cycle Management", 30 June 2020

At the beginning of the approval process, the Program Office (PO) coordinates the initial/draft PPP with the following governance authorities: Authorizing Official (AO), Trusted Systems and Networks (TSN) Focal Points, USAF Anti-Tamper (AT) Lead, and Security Management/Information Protection (IP). Please note that the program office should work closely with each of the authorities on creating PPP content well in advance of requesting an approval. For final approval, the PPP is coordinated and protected per data classification level contained within, as per Table 1-1, based on the appropriate Milestone Decision Authority (MDA).

Table 1-1   PPP Coordination and Approval

Milestone Decision Authority	Coordination
Defense Acquisition Executive (DAE)	Route the initial/draft of the PPP for review/coordination with stakeholders internal and external (e.g., AO, TSN, USAF AT Lead, and IP) to the PEO. Submit the PPP to the PEO/PEG to initiate Air Staff coordination through SAF/AQ for Air Staff 3-letter coordination to Deputy Assistant SecDef/Systems Engineering (DASD/SE) in accordance with Office of the Secretary of Defense (OSD) direction no less than 45 days prior to the Defense Acquisition Board (DAB) for OSD review of initial PPP. Submit the PPP to the PEO/PEG for Air Staff coordination through SAF/AQ for Headquarters Air Force (HAF) staffing (Service Acquisition Executive (SAE) concurrence requires 30-day lead-time). Route the SAE-signed PPP to OSD for Final PPP review and approval.
Service Acquisition Executive (SAE)	Route the initial/draft of the PPP for review/coordination with stakeholders internal and external (e.g., AO, TSN, USAF AT Lead, and IP) to the Program Executive Officer (PEO). Submit the PPP to the PEO/PEG to initiate Air Staff coordination through SAF/AQ. PEO coordinates and submits the PPP through SAF/AQ for Air Staff 2 and 3-letter coordination.
Program Executive Officer (PEO)	Route the initial/draft of the PPP for review/coordination with stakeholders internal and external (e.g., AO, TSN, USAF AT Lead, and IP) to the PEO. PEO reviews and approves the PPP.

2.0. USAF SSE CYBER WORKFLOW PROCESS.

Figure 2 depicts the USAF SSE Cyber Workflow Process, herein known as the Workflow. There are three different lanes (horizontal rows) in the process (MDA/PEO, Approval Authorities, and Government lead Program Team). These lanes represent responsibility for the activities. The process is iterative and outlines specific activities to be completed for the following sections (vertical columns):

- Acquisition Strategy.
- Request for Proposal (RFP).
- Contract Award.
- Program Execution, Program Reviews & Technical Reviews.
- Verification & Validation (V&V).
- Operations and Support.

2.1. How to Use the USAF SSE Cyber Workflow Process Chart

The blocks within the Workflow Process Chart are numbered to correspond with the Sections above (i.e., block 2.1 "Requirements Analysis" is part of Section 2.0 "Request for Proposal"). This numbering system is then carried through to Table 2 later in the document where each block in the Workflow Process Chart is further decomposed into process activities (i.e., 2.1 "Requirements Analysis" includes process activity 2.1.1 "Finalize Contractor Requirements").

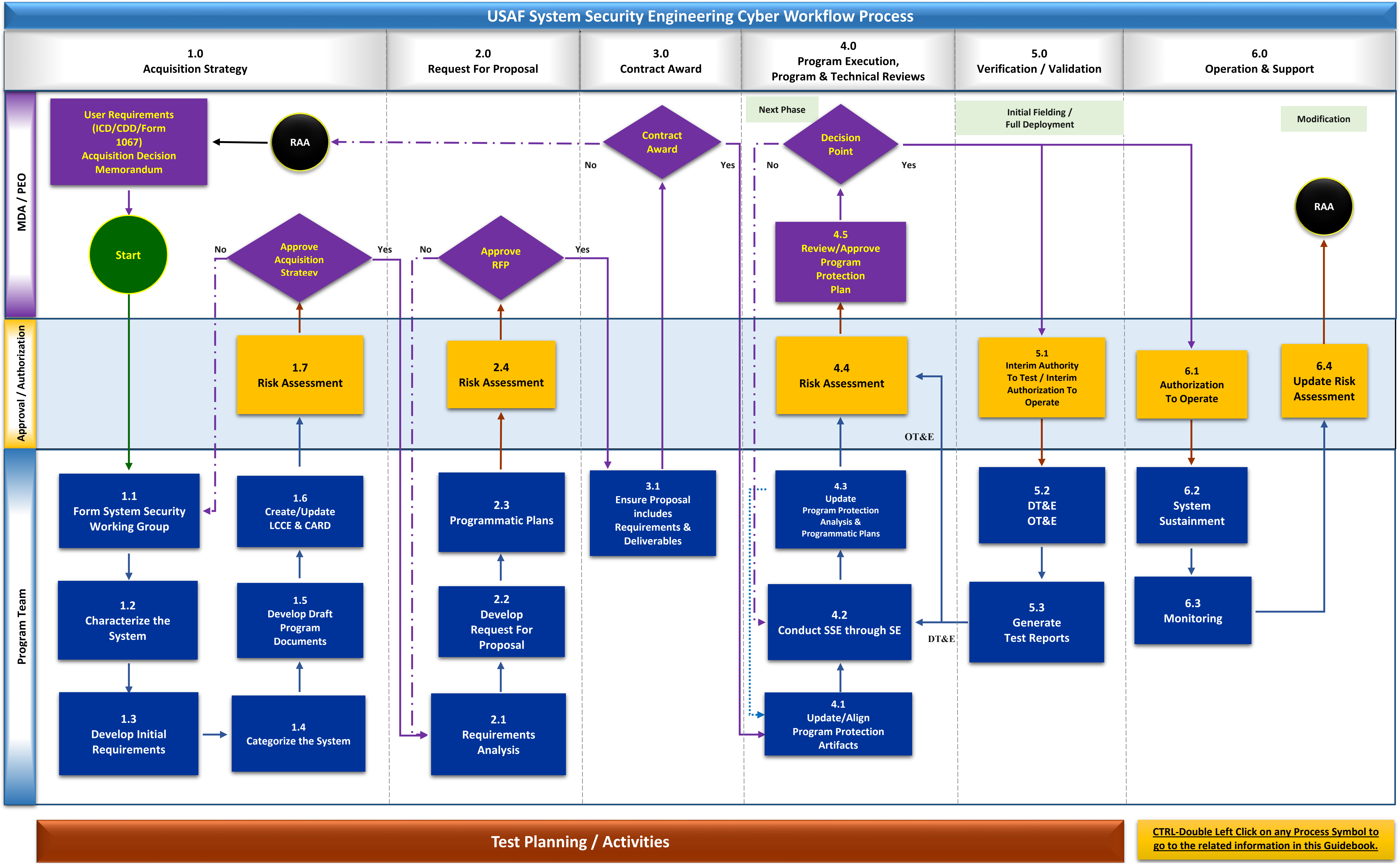

USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
RAA
Contract Award
No
Yes
Next Phase
Decision Point
No
Yes
Initial Fielding / Full Deployment
Modification
Start
No
Approve Acquisition Strategy
Yes
No
Approve RFP
Yes
4.5 Review/Approve Program Protection Plan
RAA
1.7 Risk Assessment
2.4 Risk Assessment
4.4 Risk Assessment
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
OT&E
1.1 Form System Security Working Group
1.6 Create/Update LCCE & CARD
2.3 Programmatic Plans
3.1 Ensure Proposal includes Requirements & Deliverables
4.3 Update Program Protection Analysis & Programmatic Plans
5.2 DT&E OT&E
6.2 System Sustainment
1.2 Characterize the System
1.5 Develop Draft Program Documents
2.2 Develop Request For Proposal
4.2 Conduct SSE through SE
DT&E
5.3 Generate Test Reports
6.3 Monitoring
1.3 Develop Initial Requirements
1.4 Categorize the System
2.1 Requirements Analysis
4.1 Update/Align Program Protection Artifacts
Test Planning / Activities
CTRL-Double Left Click on any Process Symbol to go to the related information in this Guidebook.

Figure 2 USAF SSE Cyber Workflow Process Chart

3.0. USAF SSE CYBER WORKFLOW PROCESS AND THE ACQUISITION LIFE CYCLE.

The Workflow should be applied continually throughout the acquisition life cycle (Figure 3 through Figure 9) and as many times as necessary to stay current with changes in the program, system design or threats that would invoke a reassessment of the cyber risks. Figure 4 highlights that the process is initiated through receiving a User requirements document.

The User requirements may be in the form of an Information Security Initial Capabilities Document (IS-ICD), Information Security Capabilities Development Document (IS-CDD), AF Form 1067, "Modification Proposal", or an Acquisition Decision Memorandum (ADM). Requirements from the IS-ICD and IS-CDD will be developed per the Joint Capabilities Integration Development System (JCIDS) process, driving the mandate to satisfy the required JCIDS Manual's Cyber Survivability Key Performance Parameter (KPP) and its associated ten Cyber Survivability Attributes (CSA).

These CSAs are part of the System Survivability Key Performance Parameter (KPP), which is one of the four mandatory KPPs listed in the Manual for the Operation of the JCIDS. CSA's are system capabilities, which support and serve as indicators of Cyber Survivability. More information on the User requirements and the CSAs can be found in **Appendix A: USAF SSE Acquisition Guidebook**.

The SSE Cyber Workflow Process can be used for a new space or weapon system development or a modification to an existing space or weapon system. The need to reapply the SSE Cyber Workflow Process within this SSECG is dependent on the Acquisition Strategy, Request for Proposal (RFP), and contract language. The Acquisition Strategy informs the criteria for the Milestone Decisions and Decision Points.

The following is an example why a program should re-evaluate and re-run the Cyber Workflow Process:

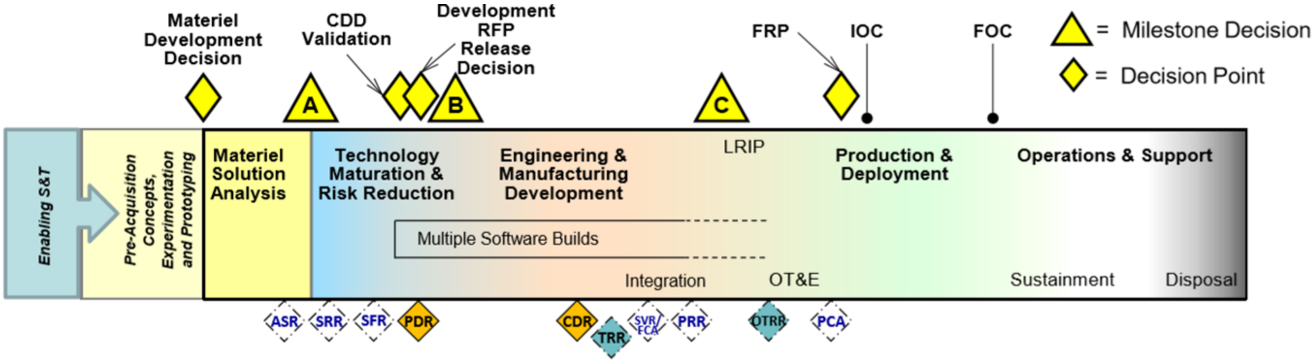
After step 4.5 of Figure 2 (also see Figure 7), the "Milestone Decision/Decision Point" leads to the V&V, initial fielding/full deployment, or the next program phase. For example, a program may have been executing this process in the Technology Maturation and Risk Reduction Phase (TMRR) and successfully passed Preliminary Design Review (PDR) and/or Milestone (MS) B, allowing the program to proceed to the Engineering and Manufacturing Development Phase (EMD).

At this point, the program should re-evaluate the acquisition strategy, ensure that the appropriate expertise is included in the Systems Security Working Group (SSWG), and continue progressing through the Cyber Workflow Process all over again. Simply put, the Cyber Workflow Process is an iterative process that is applied throughout the Space and Weapon System lifecycle.

Typically, the program will have an EMD contract awarded and the program will have to leverage the lessons learned from the previous MS, and place the proper requirements under contract.

> **NOTE:** The following figures depict the acquisition lifecycle of a Major Capability Acquisition[3] program that the SSECG can be adapted and applied to the AAF.

[3] DoDI 5000.85


Materiel Development Decision
CDD Validation
Development RFP Release Decision
FRP
IOC
FOC
= Milestone Decision
= Decision Point
A
B
C
Enabling S&T
Pre-Acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Production & Deployment
Operations & Support
Multiple Software Builds
Integration
OT&E
Sustainment
Disposal
ASR
SRR
SFR
PDR
CDR
TRR
SVR/FCA
PRR
OTRR
PCA

ASR	Alternative Systems Review	PCA	Physical Configuration Audit
CDR	Critical Design Review	PDR	Preliminary Design Review
FCA	Functional Configuration Audit	PRR	Production Readiness Review
FOC	Full Operational Capability	SFR	System Functional Review
FRP	Full-Rate Production	SRR	System Requirements Review
IOC	Initial Operational Capability	SVR	System Verification Review
OTRR	Operational Test Readiness Review	TRR	Test Readiness Review

◆ Mandatory technical reviews

◇ Best practice technical reviews and audits

◆ Test reviews

Figure 3 Acquisition Life Cycle

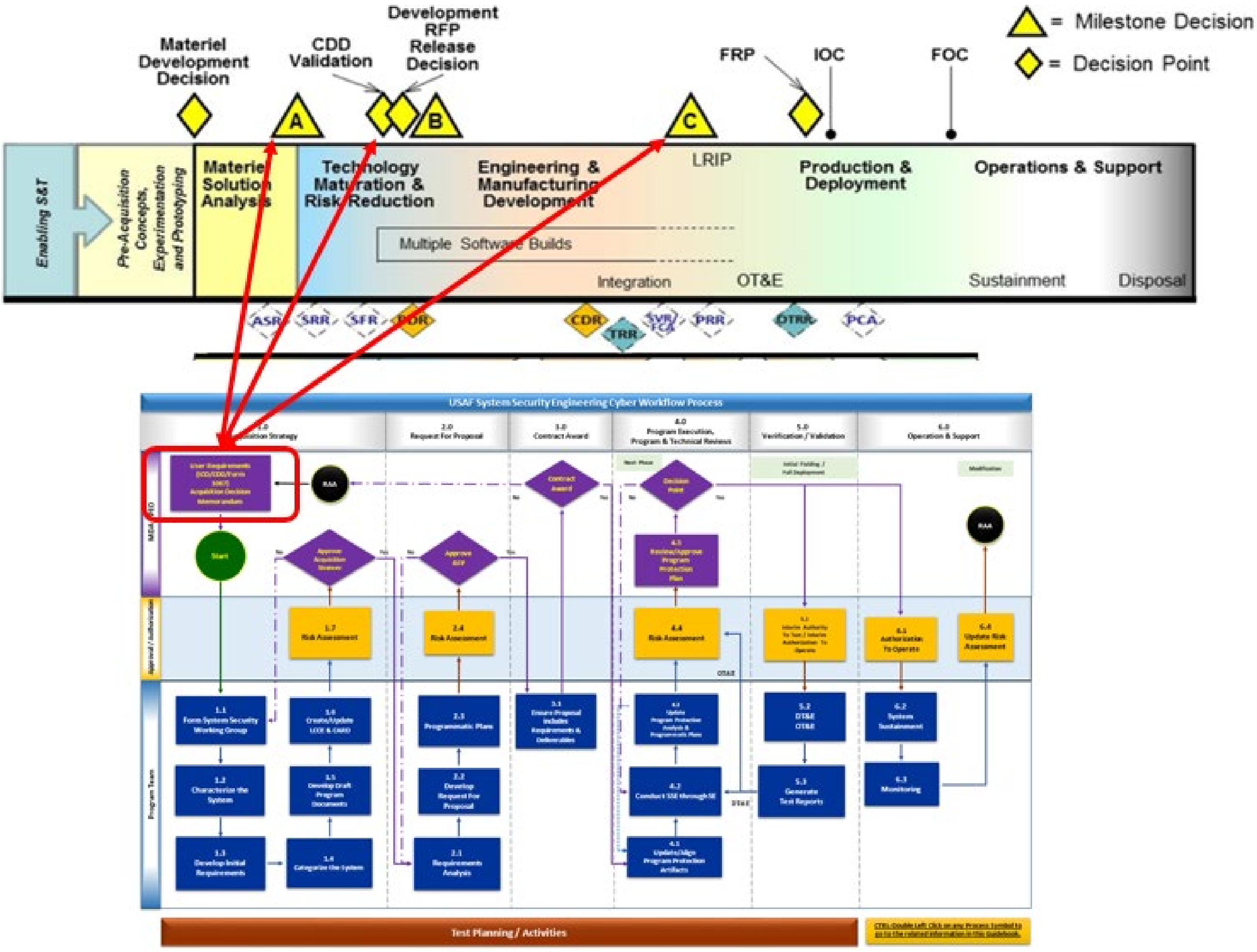


Figure 4 Requirements Aligned to Acquisition Life Cycle

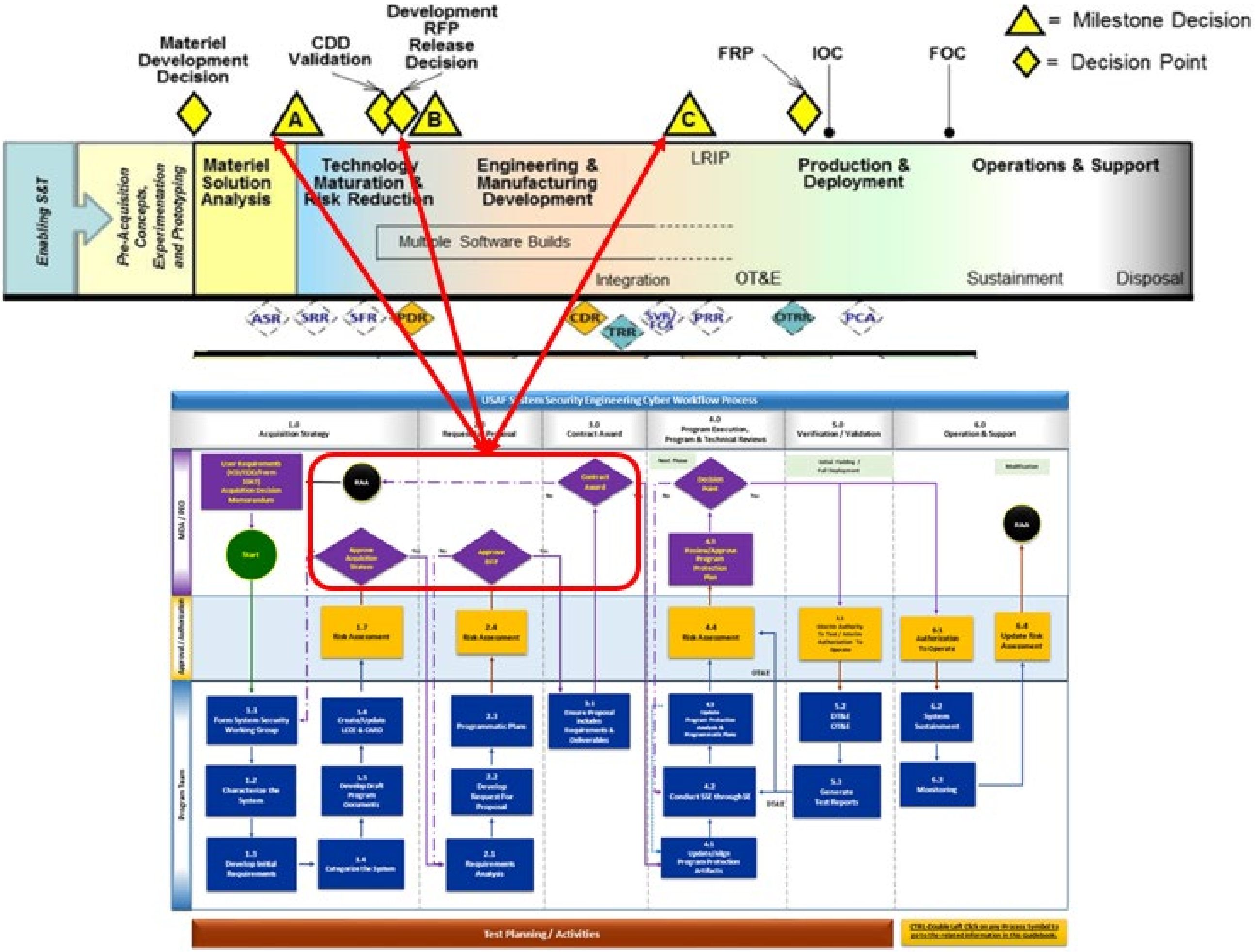

Materiel Development Decision
CDD Validation
Development RFP Release Decision
FRP
IOC
FOC
= Milestone Decision
= Decision Point
A
B
C
Enabling S&T
Pre-Acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Production & Deployment
Operations & Support
Multiple Software Builds
Integration
OT&E
Sustainment
Disposal
ASR
SRR
SFR
PDR
CDR
TRR
SVR FCA
PRR
OTRR
PCA
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request for Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
Start
RAA
Approve Acquisition Strategy
Approve RFP
Contract Award
Next Phase
Decision Point
Initial Fielding / Full Deployment
Modification
Yes
No
1.7 Risk Assessment
2.4 Risk Assessment
4.5 Review/Approve Program Protection Plan
4.4 Risk Assessment
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
1.1 Form System Security Working Group
1.2 Characterize the System
1.3 Develop Initial Requirements
1.4 Categorize the System
1.5 Develop Draft Program Documents
1.6 Create/Update LCCE & CARD
2.1 Requirements Analysis
2.2 Develop Request For Proposal
2.3 Programmatic Plans
3.1 Ensure Proposal Includes Requirements & Deliverables
4.1 Update/Align Program Protection Artifacts
4.2 Conduct SSE through SE
4.3 Update Program Protection Analysis & Programmatic Plans
OT&E
DT&E
5.2 DT&E OT&E
5.3 Generate Test Reports
6.2 System Sustainment
6.3 Monitoring
Test Planning / Activities
CTRL-Double Left Click on any Process Symbol to go to the related information in this Guidebook.

Figure 5 AS, RFP, & Contract Award Aligned to Acquisition Life Cycle

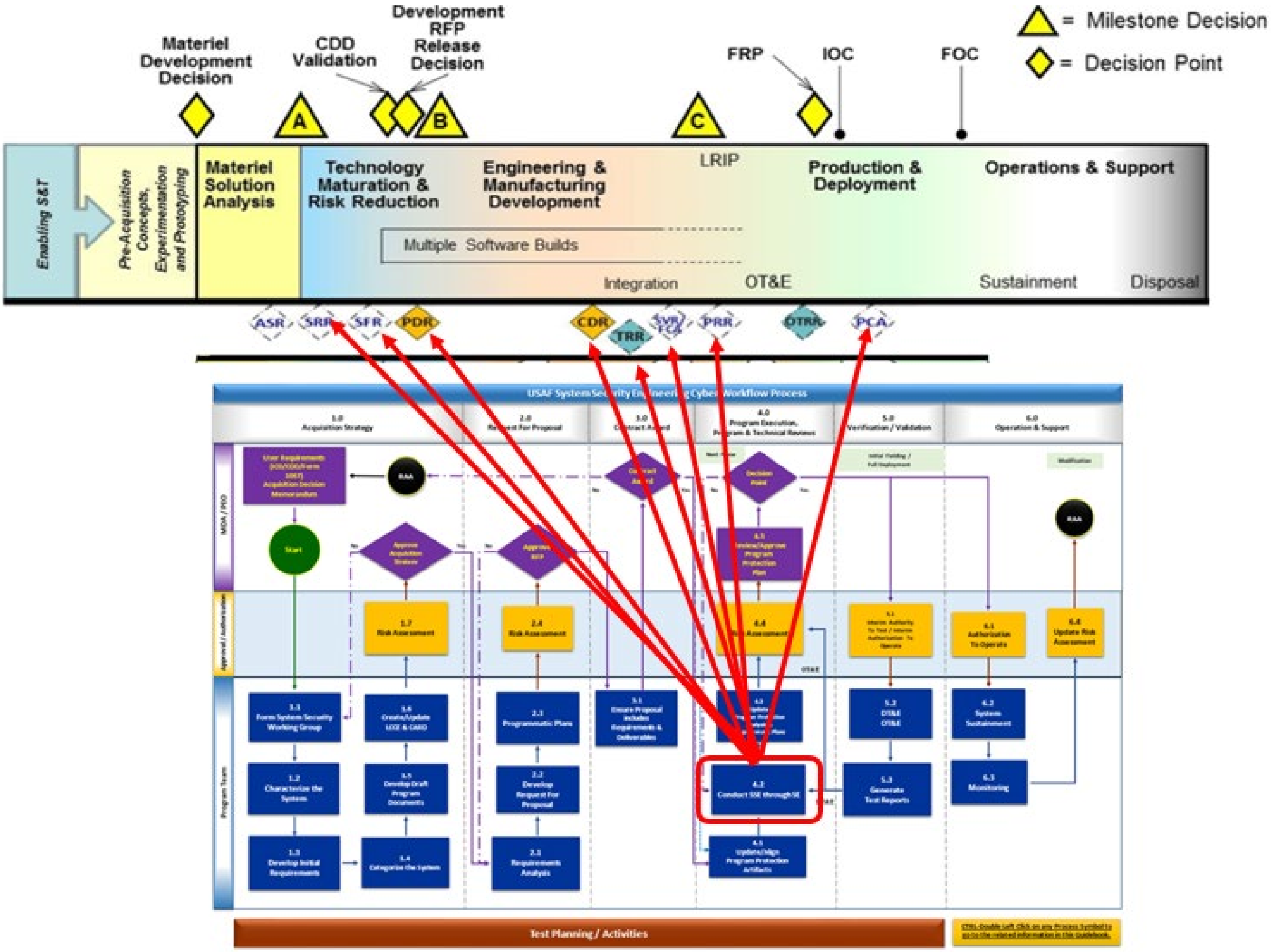

Materiel Development Decision
CDD Validation
Development RFP Release Decision
FRP
IOC
FOC
= Milestone Decision
= Decision Point
A
B
C
Enabling S&T
Pre-Acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Production & Deployment
Operations & Support
Multiple Software Builds
Integration
OT&E
Sustainment
Disposal
ASR
SRR
SFR
PDR
CDR
TRR
SVR FCA
PRR
OTRR
PCA
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
Start
RAA
Approve Acquisition Strategy
Approve RFP
Contract Award
Decision Point
4.5 Review/Approve Program Protection Plan
1.7 Risk Assessment
2.4 Risk Assessment
4.4 Risk Assessment
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
1.1 Form System Security Working Group
1.2 Characterize the System
1.3 Develop Initial Requirements
1.4 Categorize the System
1.5 Develop Draft Program Documents
1.6 Create/Update LCCE & CARD
2.1 Requirements Analysis
2.2 Develop Request For Proposal
2.3 Programmatic Plans
3.1 Ensure Proposal includes Requirements & Deliverables
4.1 Update/Align Program Protection Artifacts
4.2 Conduct SSE through SE
5.2 OT&E OT&E
5.3 Generate Test Reports
6.2 System Sustainment
6.3 Monitoring
OT&E
Test Planning / Activities

Figure 6   Conducting SSE through SE Aligned to Acquisition Life Cycle

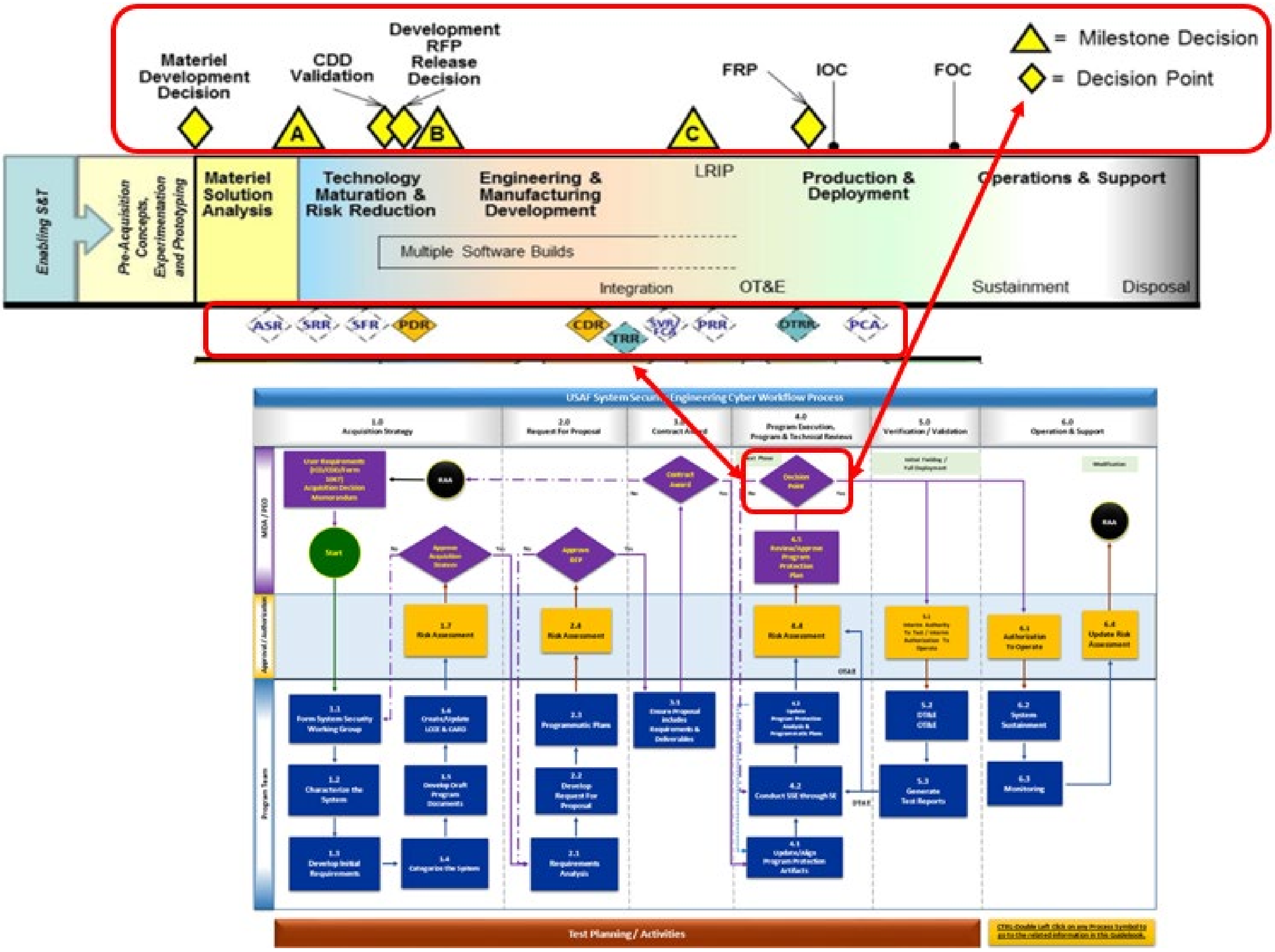

Materiel Development Decision
CDD Validation
Development RFP Release Decision
A
B
C
FRP
IOC
FOC
= Milestone Decision
= Decision Point
Enabling S&T
Pre-Acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Production & Deployment
Operations & Support
Multiple Software Builds
Integration
OT&E
Sustainment
Disposal
ASR
SRR
SFR
PDR
CDR
TRR
SVR/FCA
PRR
OTRR
PCA
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
RAA
Start
Approve Acquisition Strategy
Approve RFP
Contract Award
Decision Point
No
Yes
1.7 Risk Assessment
2.4 Risk Assessment
4.4 Risk Assessment
4.5 Review/Approve Program Protection Plan
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
Initial Fielding / Full Deployment
Modification
1.1 Form System Security Working Group
1.2 Characterize the System
1.3 Develop Initial Requirements
1.4 Categorize the System
1.5 Develop Draft Program Documents
1.6 Create/Update LCCE & CARD
2.1 Requirements Analysis
2.2 Develop Request For Proposal
2.3 Programmatic Plans
3.1 Ensure Proposal includes Requirements & Deliverables
4.1 Update/Align Program Protection Artifacts
4.2 Conduct SSE through SE
4.3 Update Program Protection Analysis & Programmatic Plans
5.2 OT&E OT&E
5.3 Generate Test Reports
6.2 System Sustainment
6.3 Monitoring
OT&E
Test Planning / Activities
CTRL-Double Left Click on any Process Symbol to go to the related information in this Guidebook.

Figure 7 Milestone Decisions/Decision Points Aligned to Acquisition Life Cycle

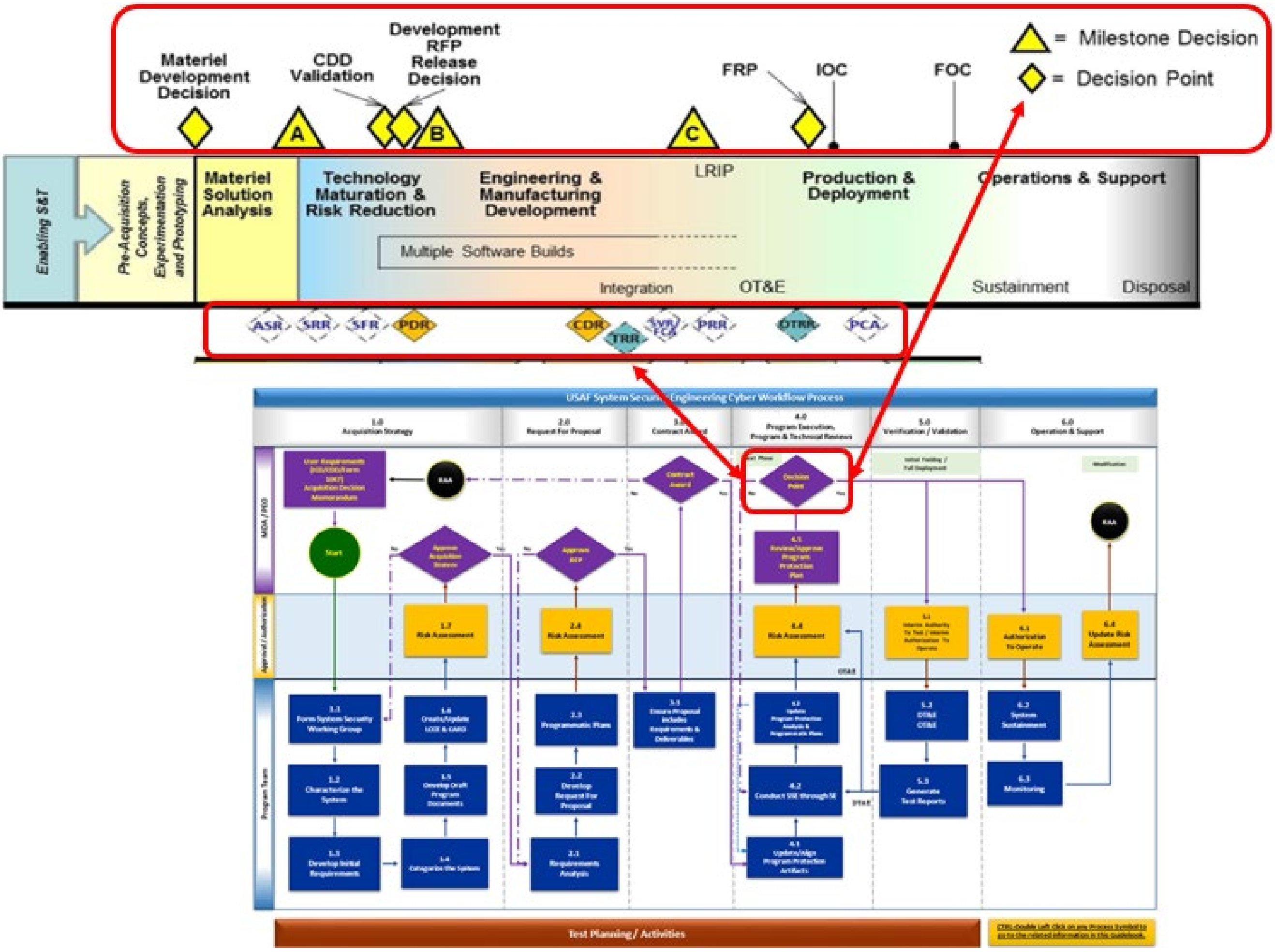

Materiel Development Decision
CDD Validation
Development RFP Release Decision
FRP
IOC
FOC
A
B
C
= Milestone Decision
= Decision Point
Enabling S&T
Pre-Acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Production & Deployment
Operations & Support
Multiple Software Builds
Integration
OT&E
Sustainment
Disposal
ASR
SRR
SFR
PDR
CDR
TRR
SVR/FCA
PRR
OTRR
PCA
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
RAA
Start
Approve Acquisition Strategy
Approve RFP
Contract Award
Decision Point
No
Yes
4.5 Review/Approve Program Protection Plan
Initial Fielding / Full Deployment
Modification
1.7 Risk Assessment
2.4 Risk Assessment
4.4 Risk Assessment
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
1.1 Form System Security Working Group
1.2 Characterize the System
1.3 Develop Initial Requirements
1.4 Categorize the System
1.5 Develop Draft Program Documents
1.6 Create/Update LCCE & CARD
2.1 Requirements Analysis
2.2 Develop Request For Proposal
2.3 Programmatic Plans
3.1 Ensure Proposal includes Requirements & Deliverables
4.1 Update/Align Program Protection Artifacts
4.2 Conduct SSE through SE
4.3 Update Program Protection Analysis & Programmatic Plans
5.2 DT&E OT&E
5.3 Generate Test Reports
6.2 System Sustainment
6.3 Monitoring
OT&E
Test Planning / Activities
CTRL-Double Left click on any Process Symbol to go to the related information in this Guidebook.

Figure 8 Test and Evaluation Aligned to Acquisition Life Cycle

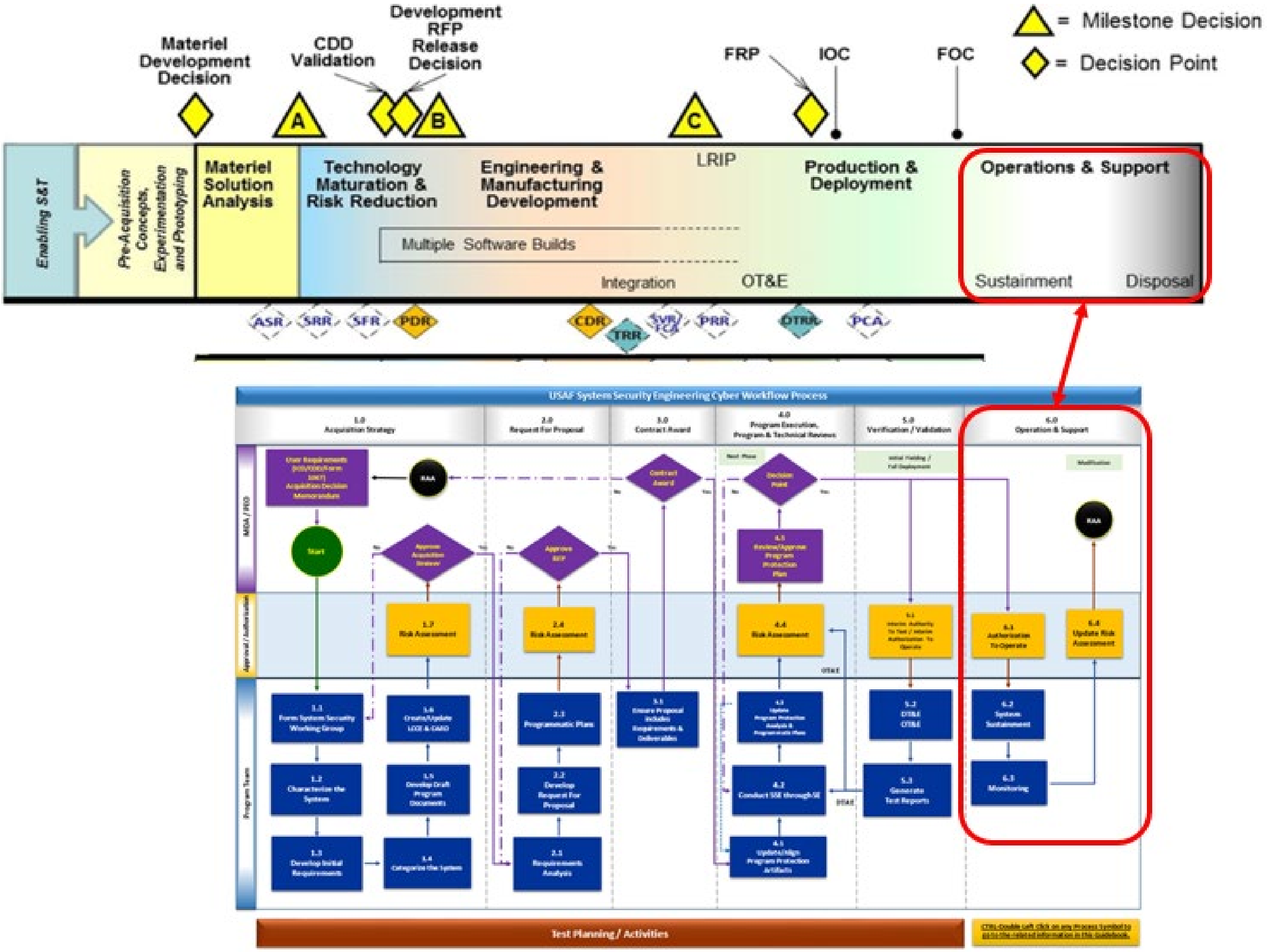

Materiel Development Decision
CDD Validation
Development RFP Release Decision
FRP
IOC
FOC
= Milestone Decision
= Decision Point
A
B
C
Enabling S&T
Pre-Acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Production & Deployment
Operations & Support
Multiple Software Builds
Integration
OT&E
Sustainment
Disposal
ASR
SRR
SFR
PDR
CDR
TRR
SVR/FCA
PRR
OTRR
PCA
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
RAA
Start
Approve Acquisition Strategy
Approve SEP
Contract Award
Decision Point
Next Phase
Initial Fielding / Full Deployment
Modification
No
Yes
1.7 Risk Assessment
2.4 Risk Assessment
4.4 Risk Assessment
4.5 Review/Approve Program Protection Plan
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
1.1 Form System Security Working Group
1.2 Characterize the System
1.3 Develop Initial Requirements
1.4 Categorize the System
1.5 Develop Draft Program Documents
1.6 Create/Update LCCE & CARD
2.1 Requirements Analysis
2.2 Develop Request For Proposal
2.3 Programmatic Plans
3.1 Ensure Proposal Includes Requirements & Deliverables
4.1 Update/Align Program Protection Artifacts
4.2 Conduct SSE through SE
4.3 Update Program Protection Analysis & Programmatic Plans
5.2 DT&E OT&E
5.3 Generate Test Reports
6.2 Systems Sustainment
6.3 Monitoring
DT&E
OT&E
Test Planning / Activities
CTRL-Double Left click on any Process Symbol to go to the related information in this Guidebook.

Figure 9 Operations & Support Aligned to Acquisition Life Cycle

3.1. SSE Cyber Workflow Process and Adaptive Acquisitions Framework

DoDI 5000.02, “Operation of the Adaptive Acquisition Framework (AAF)”, allows the Program Manager (PM) to develop a specific/tailored acquisition strategy for obtaining Milestone Decision Authorities (MDA), approval matching the acquisition pathway (Figure 10) processes, reviews, documents, and metrics to the character and risk of the capability being acquired.

DoDI 5000.02, Section 4.1, paragraph b (3) states that regardless of the acquisition pathway being used, PMs will still address cyber risks early and continuously to ensure fielded systems are cyber resilient:

“In addition, PMs will:

(3) Recognize that Cybersecurity is a critical aspect of program planning. It must be addressed early and continuously during the program life cycle to ensure Cybersecurity operational and technical risks are identified and reduced and that fielded systems are capable, effective, and resilient.”

Joint Military Requirements:

Programs seeking to use alternatives acquisition pathways to satisfy joint military requirements are subject to the JCIDS Manual, and must coordinate with the Joint Staff to assess for joint equity.

DoDI 5000.02 also clearly emphasizes in its depiction of the acquisition pathways that cyber defenses are still a top priority and are not intended to be bypassed in order to “go faster”. See the vertical red band in Figure 10, taken directly from DoDI 5000.02.

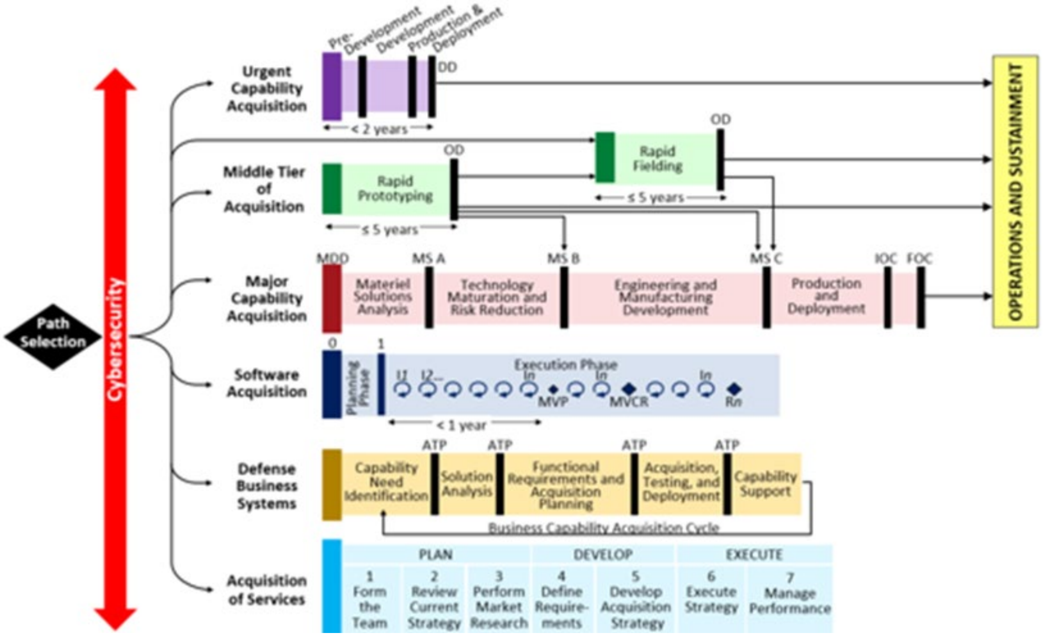

Path Selection
Cybersecurity
Urgent Capability Acquisition
Pre-Development
Development
Production & Deployment
DD
< 2 years
Middle Tier of Acquisition
Rapid Prototyping
OD
≤ 5 years
Rapid Fielding
OD
≤ 5 years
Major Capability Acquisition
MDD
MS A
MS B
MS C
IOC
FOC
Materiel Solutions Analysis
Technology Maturation and Risk Reduction
Engineering and Manufacturing Development
Production and Deployment
Software Acquisition
0
1
Planning Phase
Execution Phase
I1
I2...
In
MVP
MVCR
Rn
< 1 year
Defense Business Systems
ATP
ATP
ATP
ATP
Capability Need Identification
Solution Analysis
Functional Requirements and Acquisition Planning
Acquisition, Testing, and Deployment
Capability Support
Business Capability Acquisition Cycle
Acquisition of Services
PLAN
DEVELOP
EXECUTE
1 Form the Team
2 Review Current Strategy
3 Perform Market Research
4 Define Requirements
5 Develop Acquisition Strategy
6 Execute Strategy
7 Manage Performance
OPERATIONS AND SUSTAINMENT

Figure 10   AAF (from DoDI 5000.02)

The SSECG allows tailoring as needed for the unique needs of the selected pathway. It is highly recommended, however, the main elements of the SSE Cyber Workflow Process be retained, as Cybersecurity, Cyber Resiliency, and Cyber Survivability are very difficult, if not impossible, to achieve if not originally designed into the Defense Business System's (DBS) and Weapon System architectures. The Cybersecurity requirements differ according to the selected pathway and are noted in the following Sections ensuring statutory and regulatory compliance. SSE Cyber Workflow Process key elements are identifying the SSE requirements early, establishing SSE requirements in the contract, and utilizing adequate technical reviews to verify the system design meets the SSE requirements during development.   Shortcutting cyber protections or SSE requirements to meet the schedule timelines of rapid fielding and prototyping fail to achieve the DoD goals and expectations for cyber resilient systems outlined in AAF.

3.2. SSE Cyber Workflow Process and the Systems Engineering “V”.

The Systems Engineering (SE) “V” in Figure 11 is the engineering approach for progressing through the acquisition life cycle. Section 4.0 in the WBS decomposes PP, SSE, and SE activities to be accomplished during the acquisition life cycle. Completing SSE through the SE process is critical to ensuring Cybersecurity and Cyber Resiliency is obtained and maintained through the life cycle of a program.

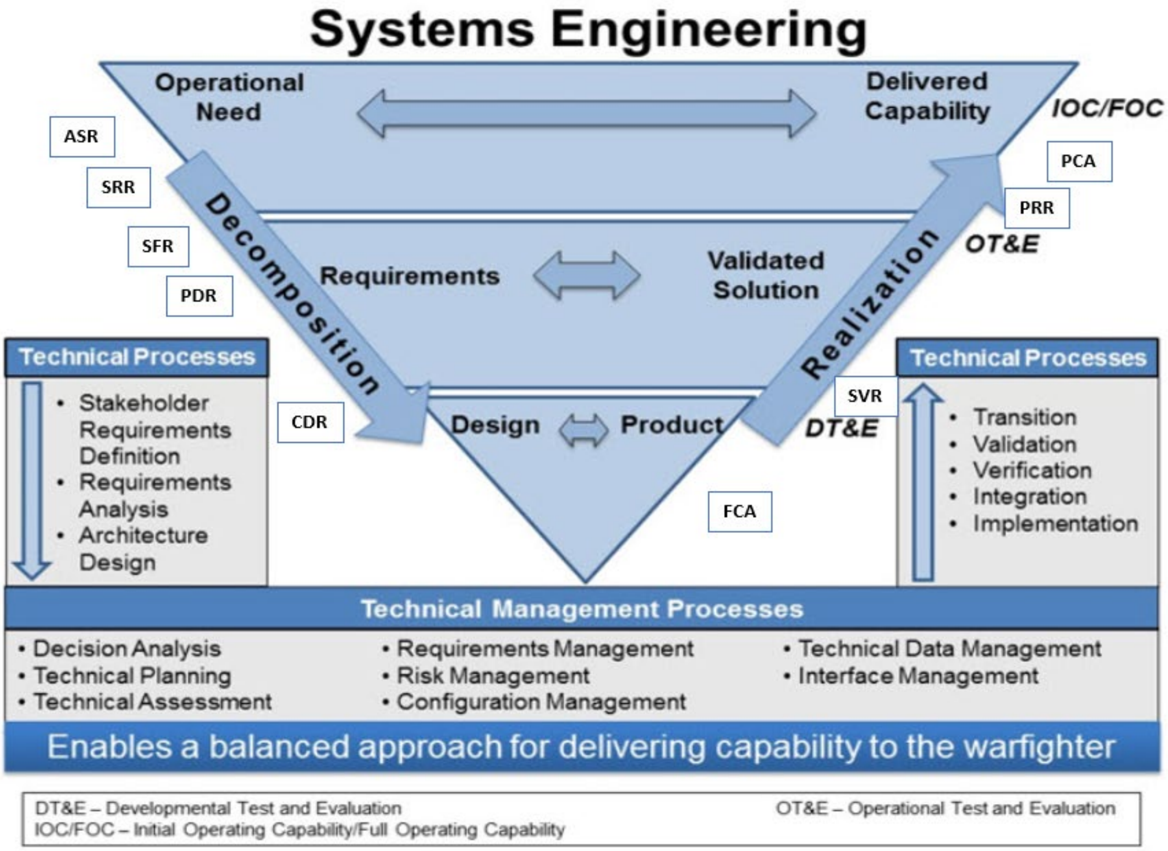


Figure 11 Systems Engineering “V”

4.0. WORK BREAKDOWN STRUCTURE.

The Work Breakdown Structure (WBS) in **Table 2** provides additional detail for each of the high-level activities within the process.

- **Activity** – Individual tasks to be accomplished.
- **Description** – Details on how to execute each activity.
- **Artifacts** – Documents created/updated during the execution of each activity.
- **OPR/Supplier** – Organization, team, or individual who has primary responsibility to execute or supply information for each activity.
- **References** – References for tools, documents, procedures, or other guidance to aid in completing each activity.

Table 4-1 WBS for the SSE Cyber Workflow Process

WBS	Activity	Description	Artifact	OPR/ Supplier	References
Requirements Approving Authority (RAA)	User Requirements	Form High Performance Team (HPT). Provide the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) changes required to achieve Mission Focused Cyber Hardening (MFCH) for a space and weapon system. Provide tailored Cyber Survivability Attribute (CSA) requirements per each critical space and weapon system function in accordance with the Cyber Survivability Implementation Guide.	• IS-ICD/IS-CDD/ AF Form 1067/ Acquisition Decision Memorandum	• User (MAJCOM) • Program Office • SSE	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD) • Cyber Survivability Endorsement Implementation Guide • DoD AT Desk Reference • DoD AT Technical Implementation Guide (TIG)
1.0	**Acquisition Strategy**				
START	Enter DoD Acquisition Life Cycle	Upon entering the DoD Acquisition Life Cycle for any space and weapon system development, AF Form 1067 or new contract, begin the process laid out in this WBS.			
1.1	**Form Systems Security Working Group (SSWG)**				
1.1.1	Appoint Personnel to SSWG / appropriate IPT	Assemble a team to support the program's protection planning. The size and nature of the project, program, or system will dictate the size and makeup of the protection team. Ensure a lead is appointed to guide and facilitate the SSWG efforts SSWG should include personnel that can cover these functions PM, program protection lead (security management/ information protection), logistics, chief engineer, systems engineer, systems security engineer, information system security manager (ISSM), intelligence, Defense Counter-Intelligence and Security Agency (DCSA), National Security Agency, and representatives from the Cybersecurity Working Group (CyWG), AO, TSN, USAF AT Lead, and IP. **NOTE:** The establishment of the CyWG is recommended within the Program Office and as a sub-group to the Integrated Test Team (ITT). Membership should include, as a minimum, the Chief Developmental Tester (CDT) and cyber representatives from the Operational Test Agency (OTA)/Operational Test Organization (OTO), the Lead Developmental Test Organization (LDTO), and the Functional Management Office (FMO). The CyWG is responsible for integrating and coordinating all Cybersecurity test and evaluation and supporting the Risk Management Framework assessment and authorization process. **NOTE:** It is a best practice for LDTO, OTA/OTO, and participating cyber test agency representatives on the CyWG to also be members of the SSWG.	• PPP Table 1.2-1	• PM	• DoDI 5000.83 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • AFI 99-103 • AFMAN 63-119 • AFPAM 63-113 • "Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, p.56155, 4 May 2020. • DoD Cybersecurity Test and Evaluation Guidebook • National Space Traffic Management Policy", Federal Register, Vol. 83, No. 120, Space Policy Directive 3, p. 28969, 21 June 2018. • DASD(SE) "Program Protection Plan Outline & Guidance"
1.1.2	Develop SSWG Charter	Publish a charter with the business rules for SSWG members to ensure Program Protection Planning and documentation is a focused effort based on well-defined objectives.	• SSWG Charter • PPP Section 1.2 and Table 1.2-1	• SSWG	• AFPAM 63-113
1.1.3	Gather Documentation	Collect relevant/available documentation to assist with the subsequent steps in the process. If modifying an existing system, review previously identified vulnerabilities of the system. Information Security Initial Capabilities Document (IS-ICD), Information Security Capability Development Document (IS-CDD), CONOPS, System Requirements Document (SRD), Systems Engineering Plan (SEP), top-level architecture, previous cyber test results/reports, etc.) Transparently share data, to the greatest extent possible, in its native form and require minimal	• PPP Section 1.1	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1) • AFPD 33-3 • Department of Defense (DoD) Mission Engineering (ME) Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		formatting and manipulation. All DoD data will be shared as widely as possible across the Military Services and OSD. Options to prevent data transparency should not be entertained by the Contracting Officer, Engineering Lead and Program Manager.			
1.1.4	Intelligence and Counter-intelligence Documentation	Request the appropriate threat information/products respective to the maturity of the program (i.e. Defense Intelligence Threat Library Threat Module, Technology Targeting Risk Assessment, Validated On-Line Life Cycle Threat (VOLT) Report, Air Force Office of Special Investigations (AFOSI) products, Initial Threat Environment Assessment, and Defense Security Service Threat Assessment).	• PPP Table 5.1-1	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Defense Acquisition Guide (DAG) Chapter 7 • AFPD 71-1 • DoDD 5240.02 • DoDI 5000.86, Acquisition Intelligence • DoDI O-5240.24 • AFPAM 63-113 • DoDD 5250.01 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1)
1.1.5	Conduct Critical Program Information (CPI) Analysis	Conduct the appropriate activities in order to identify, understand, and protect information about the program and information residing in the system being acquired. This includes the identification, classification, and marking of program and system information. Programs identified as having International Acquisition and Exportability (IA&E) content are to be classified, marked, and handled in according to the program SCG. It also provides the basis for a program to understand what information is associated with the program and system, as well as, the importance of that information. Information identified provides the basis for decisions on protections (or other requirements) that must be implemented for the program and the system. Refer to the DAG for additional detail.	• PPP Section 5.3.6 & Table 5.3.6-1 • Statement of Work (SOW) • DD Form 254	• SSWG	• DAG Chapter 9 • DoDM 5200.01 V1-V3 • DoDI 5220.22 CH-2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1)
1.2	**Characterize the System**				
1.2.1	User/Stakeholder Requirements and Information	Review and understand what the customer requirements, capabilities, desired effects are. (IS-ICD [CSAs], IS-CDD [CSAs], CONOPS/CONEMP, SRD, etc.). During the JCIDS document approval cycle, ensure that SSWG representation and High Performance Team (HPT) are supporting one another. The HPT provides User inputs to the Safety Critical Functions (SCFs), Mission Critical Functions (MCFs), and functions associated with CPI to inform the top-level architecture and the System Survivability Key Performance Parameter (KPP)/CSAs (Cyber Survivability Attributes) appropriately. **NOTE:** If the program is Pre- Milestone B, this step will generate information to be documented in the IS-CDD **NOTE:** The requirements need to be testable and measurable. This review is also the first step to beginning the MBCRA for test and evaluation.	• Acquisition Strategy (AS) • IS-CDD • Survivability and Vulnerability Program Plan (SVPP) [applicable to Space systems]	• User • SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD) • CJCSI 5123.01H • Cyber Survivability Endorsement Implementation Guide • DAG Chapter 3 Section 4.2.1 • AFI 99-103 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1). • “Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space
1.2.2	Develop System Description	Provide a high-level description of the system and the technology of which it is comprised. Describe the system (including system boundaries and interconnections). For all interconnections, determine requirements	• PPP Section 1.0 and Appendix E, Cybersecurity Strategy (CS)	• SSWG	• DoDI 8510.01 • AFPAM 63-113 • NIST SP800-37 Risk Management Framework for Information Systems and Organizations: A

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		needed to achieve Authorization to Operate (ATO).			System Life Cycle Approach for Security and Privacy • Appendix B: USAF Combined Process Guide for CPI and CC Identification, paragraph 5.5.1 • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
1.2.3	ID Mission Environment(s)	Identify the environments the system is planned to be operated and maintained in, to include geographical areas for deployment/operations and applicable kinetic and cyber threat environments. ME (Mission Engineering) and MIM (Mission Integration Management) activities will be performed as part of concept and system development to inform developmental decisions and ensure the department is systematically investing in the appropriate capabilities, in an integrated and cost effective manner, to meet mission needs. Include system-unique maintenance/test equipment and training systems if applicable.	• PPP Section 1.1	• SSWG	• United States Code (USC) Title 10, § 133a, 133b • DoDI 5000.88 • DoDI 5000.90 • AFI 99-103 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2) • DoD Mission Engineering Guidebook
1.2.4	Bound the System/ID System Boundary	Identify the system boundaries, interconnections/interfaces, and dependencies to include what systems are internal/external to the system boundary. Identify mission dependence that are affected by either connectivity into or out from the space and weapon system. When identifying internal and external dependencies, seek to identify content and connectivity dependencies that can adversely affect system mission, system content, or connectivity that can adversely affect the mission of a connected system. **NOTE:** Based on maturity of program, details of the internal and external boundaries may or may not be known. If unknown, ensure bounding the system is started no later than System Functional Review (SFR). System boundaries should be updated as more information becomes available.	• PPP Section 1.1 and Appendix E	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.2.5	Conduct CPI Identification/ Analysis	CPI should be identified early and reassessed throughout the life cycle of the program, to include: • Prior to each acquisition milestone • Prior to each system's engineering technical review • Prior to each phase of Cybersecurity and Cyber Resiliency testing (e.g., Phases 3 – 6) • Throughout operations and sustainment • During software/hardware technology updates. • Use applicable CPI tools, Subject Matter Expert (SME), functional decomposition, and data flows to identify candidate and final CPI, as well as, its location. Use the functional decomposition, identified boundaries and system interfaces to develop the list of critical components and determine its criticality. • Classifying CPI COC as per the AT FOUO SCG, Table Entry VI.13. • **NOTE:** PO should follow internal PEO Directorate level coordination process to request final MDA approval. *Programs without CPI are still required to do a PPP*. **NOTE:** CPI protection should commence soon after the CPI has been identified, and, like CPI identification, CPI protection should continue throughout the life cycle of the program. The PO should work with the AT office early to avoid compromised components.	• PPP Section 2.2, Table 2.2-1, Section 3.0 and Section 4.0 • Anti-Tamper Plan	• SSWG	• DoDI 5200.39 • AFPAM 63-113 • DAG Chapter 9 • DoD Critical Program Information (CPI) Horizontal Protection Guidance (HPG) • DoD Anti-Tamper Desk Reference • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis (FTA) • DoD Program Protection Plan Outline & Guidance • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
1.2.6	Functional Thread Analysis	Conduct the functional decomposition, criticality analysis, Vulnerability Analysis (VA) and generate Attack Path Vignettes (APV).	• Criticality Analysis Input, PPP, Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD, and 1.10 Risk Management) • Appendix C: Functional Thread Analysis • ISO 17666: 2016, Space Systems – Risk Management, 1st ed. • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.6.1	Conduct Functional Decomposition	Decompose the system beginning with the highest-level User requirements. Identify the system-level mission critical functions, safety critical functions, and the functions associated with CPI. **NOTE:** depending on the maturity of the system, the functional decomposition will have higher fidelity. Ultimately, the system should be functionally decomposed to the individual component level.	FTA Report	SSWG	• Appendix D: Attack Path Analysis (APA)
1.2.6.1.1	Conduct Criticality Analysis	An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s). Understand the consequence associated with the MCFs, SCFs, and functions associated with CPI in accordance with Section 1.10 of Appendix A: USAF SSE Acquisition Guidebook. Additionally, identify the cyber events, manmade or natural, that will result in the	• Criticality Analysis, PPP Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD and IS-CDD, 1.10 Risk Management). • Appendix B: USAF Combined Process Guide for CPI and CC Identification. • Appendix D: Attack Path Analysis (APA). • (U) Anti-Tamper (AT) Security Classification Guide, 30 July 2020 (U//FOUO). • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2).

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		system's failure/degradation that affect the mission capabilities as specified by the Requirements Approval Authority (RAA).			• DoDI 5000.83 Tech and PP to Maintain Technological Advantage • DoDI 5000.85 Major Capability Acquisition • DoDI 5200.44 Protection of MCF to Achieve TSN • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • National Space Traffic Management Policy", Federal Register, Vol. 83, No. 120, Space Policy Directive 3, Section 2, p. 28970, 21 June 2018
1.2.6.1.2	Prioritize the Functions	Prioritize the functions based on the User requirements, risk assessments, and intended operational environment (including threats).	• Criticality Analysis Input, PPP Appendix C • FTA Report • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD, and 1.10 Risk Management) • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix C: Functional Thread Analysis (FTA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2). • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.6.2	Deleted.				
1.2.6.3	Conduct Vulnerability Analysis	Analyze inherited vulnerabilities from required system of system connections, including access points and attack paths.	• Vulnerability Analysis	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix C: Functional Thread Analysis (FTA) ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix D: Attack Path Analysis (APA) • (U) Anti-Tamper (AT) Security Classification Guide, 30 July 2020 (U//FOUO) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.6.3.1	Identify Vulnerabilities	Identify all known and potential vulnerabilities. A vulnerability is any weakness in system design, development, production, or operation that can be exploited to defeat a system's mission objectives or significantly degrade its performance (including exfiltration of data, which can be used to negatively impact mission effectiveness of the targeted system or other mission systems). All aspects must be considered to include the development, production, test, and operational environments; this includes both industry and Government locations.	• PPP Section 5.2, Table 5.2-1 • Risk Management Framework for DoD IT Plan • Inputs to Cybersecurity Risk assessment	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA). • DoDI 8500.01 • DoDI 8510.01 • AFI 17-101 • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.2.6.3.2	Analyze Entry Access Points and Attack Path Vulnerabilities	Analyze cyber Entry Access Points (EAPs) and Attack Paths. Analyze EAPs and potential cyber vulnerabilities that would allow threats to gain access to the system's CPI or CCs, or to trigger a component malfunction, failure, or inability for the system to perform its intended function. Identify potential weaknesses in the component design, architecture, or code that could be potentially exploited to negatively impact the integrity, confidentiality, and availability of system data. Identify the supply chain, development, production, and test environments and processes that would allow adversaries to exfiltrate/gain access to CPI or introduce components (hardware, software, and firmware) that could cause the system to fail at some later time. Identify potential mission impacts if identified data is compromised. Complete / update the Functional Thread Analysis per Appendix C: Functional Thread Analysis.	• Risk Management Framework for DoD IT Plan. • Inputs to Cybersecurity risk assessment. • FTA Input. • APA Input.	• SSWG • CyWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.6.3.3	Generate Attack Path Vignettes	Develop cyber-attack scenarios (i.e., Attack Path Vignettes) that combine identified potential cyber vulnerabilities into operationally representative cyber-attack paths. The Attack Path Vignettes should identify attack path nodes, methodologies, anticipated mission impacts, risk ratings, and potential test methodologies/resources.	• APA Input	• SSWG	• Appendix D: Attack Path Analysis (APA)
1.2.7	DELETED				
1.2.8	DELETED				
1.2.9	Conduct Threat Analysis	Provide supporting Acquisition Intelligence unit the known information developed in WBS 1.2. Acquisition Intelligence unit performs an updated likelihood for the overall risk assessment based on known threat data. **NOTE:** The higher the fidelity of the information provided to the Intelligence Community (e.g., component part numbers if available), the higher the fidelity and relevance of the information the Intelligence Community can provide.	• Inputs to Risk Assessment	• SSWG	• ISO 17666:2016, Space Systems – Risk Management • Appendix A: USAF SSE Acquisition Guidebook (Risk Management). • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.1	Determine Scope of Threat Assessment	Consult with SSWG to establish scope and depth of threat assessment to be performed. Identify operational scenarios and threat actors relevant to the system.	• Documentation on bounds of threat analysis to include hardware and software listings, system boundary diagrams, systems engineering drawings/ DoDAFs	• Supporting Acq Intel unit • AFOSI	• United States Code (USC) Title 10, § 133a, 133b • DoDI 5000.88 • DoDI 5000.90 • DoD Mission Engineering Guidebook • AFI 99-103 • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • WBS 1.2.3 (operational environment, deployment locations/scenarios, Acquisition Intelligence Guidebook (AIG))

WBS	Activity	Description	Artifact	OPR/ Supplier	References
					• NIST SP800-30 r1.0 Tasks 1-2 and 1-5 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.2	ID Threat Sources	Determine threat sources to be incorporated into analysis (e.g. adversary nation state, hacker community, insider, supply chain, etc.). Determine threat information sources (e.g. mine existing intelligence/counterintelligence, develop new production requirements, and identify appropriate Production Centers for each threat type).	• Documentation of threats to be considered and sources for intelligence on each threat type • PPP Sections 5.0, 5.1, Table 5.1-2 • Risk Management Framework for DoD IT Plan • Operations Security (OPSEC) Plan	• SSWG • Supporting Acq. Intel Unit • AFOSI	• DoDI 5000.88 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • DoD Mission Engineering Guidebook • AFMAN 14-401 • AFI 17-203 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0 Tasks 1-2 and 1-5
1.2.9.3	ID Threat Events	List possible ways threat sources could exploit potential and known vulnerabilities (of analogous systems).	• Risk Management Framework for DoD IT Plan • OPSEC Plan	• SSWG • Supporting Acq Intel unit • AFOSI • Defense Intelligence Agency (DIA) • National Air & Space Intelligence Center (NASIC)	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoDI 5000.86 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • AFI 63-101/20-101 • AFMAN 14-401 • NIST SP800-30 r1.0 • Adversary Cyber Threat Analysis (ACTA) Process • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.4	Conduct System Research	Research the system's operation to include its capabilities, functions, external interactions and key dependencies, CONOPS, combat environment, KPPs, etc. Determine system's cyber dependencies. Identify existing intelligence relevant to the system, its capabilities, and the cyber operational environment, taking into account adversary cyber strategy and doctrine and relevant operational scenarios. Review analysis with SSWG and refine/adjust as required. **NOTE:** Program will provide artifacts to supporting Acquisition Intelligence Unit.	• Production Requirements (PR) Record Copy	• Supporting Acq Intel Unit	• DoDI 5000.83 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • Adversary Cyber Threat Assessment (ACTA) step #15 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.5	Critical Intelligence Parameter (CIP) Breach Review	Assess the impact of changes to adversary capabilities related to the CIP and determines if the breach compromises mission effectiveness of current or future capability solution(s).	• Cyber threat risk matrices	• Supporting • Acq Intel Unit SSWG	CJCSI 5123.01H
1.2.9.6	Translate Intelligence/ Counterintelligence Risk	Use established methodologies, such as Classified Information Compromise Assessment (CICA) and its associated Damage Assessment Report (DAR) to translate Intelligence Community threat rankings to RMF-compatible risk matrices.	• Cyber threat risk matrices	• Supporting Acq Intel Unit • AFOSI	• DoDI 5000.86 • DoDI 5000.90 • DoDI 8500.01 • DoDI 8510.01 • Adversary Cyber Threat Assessment (ACTA) step #16 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0
1.2.9.7	Deliver Threat Assessment to SSWG	Provide completed forms, associated narrative, and risk transition product to the SSWG.	• Threat Assessment documentation (as required): - Cyber threat risk matrices	• Supporting Acq Intel Unit • AFOSI	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoDI 5000.88 • DoDI 5000.90

WBS	Activity	Description	Artifact	OPR/ Supplier	References
			- Overlays of cyber threats on program design documents - Cyber threat register - Production Center narrative cyber threat analyses - Associated briefings		• DoDI 8510.01 • DoDI 8500.01 • AFI 99-103 • Adversary Cyber Threat Assessment (ACTA) step #16 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.10	Unmitigated Initial Risk Assessment	The unmitigated risk assessment is necessary to allow the SSWG to examine the initial risks within the system. The depth of the unmitigated risk assessment will rely on the fidelity of program information. Identify SSE risks by pairing threat events and vulnerabilities; consider all risks to include CPI/CC/TSN/Cybersecurity and Security Management/Information Protection. Document SSE risks in the Program's Risk Register, and capture the resultant risk assessment in the MBCRA products. **NOTE:** This initial risk assessment is titled "unmitigated" because the SSWG has not established any SSE requirements or mitigations based off the known information at this given point in development. Some SSE considerations may be documented in the User requirements, and those will be further decomposed to mitigate any risks identified in this step and hereafter.	• Risk Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix C: Functional Thread Analysis (FTA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.10.1	Develop Initial Recommendations	Develop initial set of recommendations that address identified potential cyber vulnerabilities. Evaluate and provide recommendations for the De-Identification of data, drawings and information through a series of effective approaches, algorithms, and tools. Recommendations should include design remediations, exploitation mitigations, test support, and other assessment team recommendations that could help drive a more survivable system.	• Risk Assessment	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • NISTIR 8053, De-Identification of Personal Information
1.2.11	Draft Security Classification Guide (SCG)	Conduct appropriate information analysis in order to identify, understand and protect the information about the program that will require classification, and marking considerations. Incorporate the Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems. **NOTE:** Ensure SCG addresses functional test plans, cyber test plans, test reports, and vulnerability information/findings, to include potential vulnerability information contained in the MBCRA.	• PPP, Appendix A (SCG)	• SSWG	• DoDI 5200.48 • Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems
1.3	**Develop Initial Requirements**				
1.3.1	Conduct Trade Space Analysis	The SSWG conducts a trade space analysis of cost, schedule, and performance for the prioritized MCFs, SCFs, and functions associated with CPI to inform the top-level architecture and the System Survivability KPP/CSAs appropriately.	• Criticality Analysis Input, PPP Appendix C	• SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (1.1.2 HPT (High Performance Team) Implementation of JCIDS Survivability KPP and CSAs)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Trade Space Analysis in: • Producing more complete and robust requirements pre-Milestone A • Making the engineering design process much more efficient and effective • Considering the manufacturability of a proposed design explicitly • Establishing baseline Cyber Resiliency of current capabilities These alternatives are then compared to the Critical Functions of the system to evaluate the risks versus the value of requirement decisions derived from the Trade Space Analysis. These decisions drive the architecture's system boundaries (internal and external) with emphasis on protection of the MCFs, SCFs and functions associated with CPI. These in turn drive the need for repeating a FTA the MCFs and SCFs and their criticality may have changed. **NOTE:** Based on maturity of program, details of the internal and external boundaries may or may not be known.	• Initial Concept Design Review (ICDR) • Survivability and Vulnerability Program Plan (SVPP)		• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DASD (SE)/DoD CIO Trusted Systems and Network Analysis • DoDI 5000.02 • DoDI 5000.88 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2) • NIST 800-160, Vol. 1 • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space, 19 July 2010
1.3.2	Develop Initial Requirements	Develop initial requirements documents (i.e., Statement Of Objectives/ Statement of Work (SOO/SOW) requirements, CDRLs (to include test support deliverables) System Requirements Document (SRD), and System Specifications Requirements). Ensure adequate coverage of SSE requirements and complete traceability to User Requirements / Stakeholder Requirements in WBS 1.2.1. Ensure the Security Management/Information Protection requirements are in the requirements (security clearance requirements, physical security for safeguarding information (Secure Classified Information Facility (SCIF), Special Access Program Facility (SAPF), Open storage facilities, Secret Internet Protocol Router Network (SIPRNet) terminals, storage containers), any additional security features (restricted areas, guns, gates, and guards), training, and start a draft DD 254 to provide. **NOTE:** CyWG representatives within the SSWG should confirm requirements are testable, measurable, and achievable.	• Initial SOO/SOW, SRD/Spec, or equivalent	• SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specification, 2.3 SOO and SOW, and Attachment 1) • NIST 800-160, Vol. 1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2) • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space
1.3.2.1	Assess SSE Requirements Implementation	Assess SSE Requirements Implementation using the Excel workbook in Appendix E.	• SSE Requirements Implementation Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (Attachment 1) • Appendix E: SSE Requirements Implementation Assessment
1.3.3	Submit Production Requirements	Coordinate production requirements (PRs) with supporting Acquisition Intelligence unit. Acquisition Intelligence unit will submit PR to appropriate intelligence/counterintelligence community Production Centers (DIA, NASIC, DIA-TAC, AFOSI, etc.). **NOTE:** Include production requirements for supplier threat information for identified critical components.	• PR Record Copy	• Supporting Acq Intel Unit	• DoDI 5000.83 • DoDI 5000.86 • DoDI 5000.90 • DoDI 8500.01 • DoDI 8510.01 • Adversary Cyber Threat Assessment (ACTA) step #15 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0
1.4	**Categorize System**				
1.4.1	Identify Critical System Information	Identify and document all the types of information processed, stored, or transmitted by the system and determine their security impact values.	• PPP Appendix E, Cybersecurity Strategy (CS) • Information Technology (IT) Determination or	• PM/Information Security Officer (ISO) • Information System Security	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • CNSSI No. 1253 • DAG Chapter 9

WBS	Activity	Description	Artifact	OPR/ Supplier	References
			Categorization Document	Manager (ISSM)	• DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.4.2	Categorize	Determine and document the confidentiality, integrity and availability (C-I-A) levels. Verify the controls determined, per C-I-A level and AO overlay, are accounted for in the system requirements per Appendix A: SSE AG Attachment 1. Prepare and submit IT Categorization and Selection Checklist for AO approval.	• PPP Appendix E, Cybersecurity Strategy • IT Determination or Categorization Document	• PM • Information Systems Security Officer (ISSO) • ISSM • AO or designee	• Appendix A: USAF SSE Acquisition Guidebook (Attachment 1) • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • AFI 17-101 • CNSSI No. 1253 • NIST SP800-53 v5 • NIST SP800-37 • Federal Information Processing Standards (FIPS) Publication 199 • DoDI 8500.01 • DoDI 8510.01 • DoDI 5000.82 • USC Title 40, Clinger-Cohen Act • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
1.4.3	Cybersecurity Strategy (CS)	Submit the Cybersecurity Strategy (CS) in accordance with the Clinger-Cohen Act. **NOTE:** The Cyber Test Strategy is captured in the TEMP and summarized in the CS in the “Cybersecurity Testing” Section. The CS shall identify the Testing Integration and Product Evaluation along with the Cryptographic Certification items being incorporated into the system design. The CS also provides the program test ISSP, Number 11 (undated) and the NSA and NIST related certification item testing elements.	• PPP Appendix E, Cybersecurity Strategy	• PM • ISSO • ISSM • AO or designee • CyWG • Test Agencies	• Appendix C: Functional Thread Analysis (FTA) • DoDI 5000.90 • AFI 17-101 • AFMAN 17-1402 • CNSSI No. 1253 • NIST SP800-37 • DoDI 8500.01 • DoDI 8510.01
1.4.4	Register System	Register information systems and Platform Information Technology (PIT) systems, IAW DoDI 8510.01 and AFI 17-101, in Information Technology Investment Portfolio Suite (ITIPS) and Enterprise Mission Assurance Support Service (eMASS).	• eMASS • ITIPS	• PM • ISSO • ISSM	• NIST SP800-37 • DoDI 8510.01 • AFI 17-101 • AFI 17-130
1.5	**Develop Draft Program Documents**				
1.5.1	Intelligence and Counterintelligence Requirements and Documentation	Request, from your program office’s assigned Acquisition Intelligence representative, the appropriate threat information/products respective to the maturity of the program, (e.g. Defense Intelligence Threat Library Threat Modules, Technology Targeting Risk Assessment, Validated On-line Life-cycle Threat (VOLT) Report, AFOSI products (as listed in PPP Outline and Guidance V1.0, Section 5.1 and 6.0) and Defense Security Service Threat Assessment).	• PPP Table 5.1-1	• SSWG	• DAG Chapter 7 • DoDI 5000.86 • DoDI 5000.90 • DoDD 5240.02 • DoDI O-5240.24 • AFPAM 63-113 • DoDD 5250.01

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.5.2	Foreign Participation	Draft Technology Assessment/Control Plan (TA/CP); consider and develop Foreign Military Sales (FMS) strategy with CPI/CC protection decisions moving forward with the Protection Strategy. Consider customization of Defense Exportability Features (DEF) if there is a potential to sell an export variant to a foreign customer in the future.	• PPP Section 8.0 • TA/CP	• PM	• AFI 10-701 • AFI 10-701, AFSC Supplement • AFI 63-101/20-101 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • AT Technical Implementation Guide (TIG) • DoD Anti-Tamper Security Classification Guide (SCG) • DoDI 5200.39 • DoDI 5200.44 • PPP Outline and Guidance V1.0.
1.5.3	MOVED to 1.7.5				
1.5.4	Draft Program Documents	Ensure program artifacts include SSE and cyber test considerations.	• AT Concept Plan • Test and Evaluation Master Plan (TEMP) • SEP • Information Support Plan (ISP) • Life Cycle Sustainment Plan (LCSP) • Draft Program Protection Plan (PPP)	• SSWG • CyWG	• AFI 99-103 • AFLCMC Internal Process Guide for Operational Test & Evaluation (OT&E) Readiness Certification • AFM 99-113 • Appendix A: USAF SSE Acquisition Guidebook (1.0 Programmatic Documents) • AT Plan Template • AT Technical Implementation Guide (TIG) • DAG CH 3-4.3.24 • DOT&E TEMP Guidebook • DoD Cybersecurity Test and Evaluation Guidebook
1.6	**Create/Update LCCE & CARD**	Create/update Life Cycle Cost Estimate (LCCE) & Cost Analysis Requirements Description (CARD) with costs to achieve CPI/CC/TSN/Cybersecurity and Security Management/Information Protection requirements (**WBS 1.3**) for the program.	• PPP Section 11.0, CARD, LCCE, POE	• PM/Chief Engineer/ Financial Mgmt Office	• **Appendix A: USAF SSE Acquisition Guidebook (1.5 Cost Analysis Requirements Description (CARD))** • **DoDI 5000.73, "Cost Analysis Guidance and Procedures", 13 March 2020**
1.7	**Risk Assessment**				
1.7.1	Review Criticality Analysis	Review and update criticality analysis initiated in **WBS 1.2** based on feedback from **WBS 1.3** & **WBS 1.4**, as necessary.	• PPP Appendix C • Updated Criticality Analysis	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DAG Chapter 9 • DoDI 5200.44 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.7.2	Review Vulnerability Analysis	Review and update the analysis on WBS 1.2.6.3 (vulnerabilities from required system of system connections, including access points and attack paths). **NOTE:** Depending on the maturity of the system, the vulnerability analysis should not be limited to only the system of system connections.	• Updated Vulnerability Analysis	• SSWG	• DoDI 8500.01 • DoDI 8510.01 • DoD Trusted Systems and Networks (TSN) Analysis • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.7.3	Review Threat Analysis	Review and update threat analysis initiated in WBS 1.2.9, as necessary. Threat information is based on current intelligence and counterintelligence.	• Updated Risk Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.7.4	Risk Assessment	Identify SSE risks by pairing threat events and vulnerabilities; consider all risks to include CPI/CC/TSN/Cybersecurity and Security Management/Information Protection. Document SSE risks in the Program's Risk Management Process and System Safety Process. In addition, capture the pairing of threats and vulnerabilities within the MBCRA. Obtain SSE risk approval from the appropriate approving authority (i.e. PM, PEO, SAE, or Chief Information Officer (CIO)). If risk assessment is not approved, return to previous steps necessary to mitigate the unapproved risks. Update SSE Requirements Implementation Assessment.	• Independent Technical Risk Assessment (ITRA). • Risk Assessment • SSE Requirements Implementation Assessment • Hazard Assessment	• IRTA Tea. • SSWG • System Safety Group.	• DoDI 5000.88, Engineering of Defense Systems, Section 3.5 • DoDI 5000.90 • Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Appendix E: SSE Requirements Implementation Assessment • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • AFI 91-102_AFGM2020-01 • MIL-STD-882E • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • AFLCMC Standard Process for Cybersecurity Assessment and Authorization • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.7.4.1	Generate Initial MBCRA Products	Generate FTA & APA Reports documenting identified Entry Access Points, Cyber Boundary, Cyber Attack Paths, potential cyber vulnerabilities, Mission Critical Functions, Safety Critical Functions, and potential operational impacts if the identified potential cyber vulnerabilities are exploited. Update APA for high-risk potential vulnerabilities identified during FTA risk assessment, as needed. Update CTA & cyber test methodology as needed based on any new or changed potential vulnerabilities. **NOTE:** Ensure all resources used, as well as, the analysis processes used, assumptions made, and conclusions reached during the FTA & APA analysis activities are clearly codified in program documents for later reference (particularly during future FTA & APA updates). Resources used for these analyses should be stored in a single resource repository.		• CyWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.7.5	Risk Management	Integrate risks associated with CPI/CC/TSN/ Cybersecurity and Security Management / Information Protection with the Program Risk Management process. As these risks are identified and managed, they should be included when risks are briefed up the chain of command. **NOTE:** Appropriately classify, mark, and handle security risks.	• Independent Technical Risk Assessment (ITRA). • Program Protection • Acquisition Strategy Panel (ASP) slide (coordination with ACE) • Risk Register	• IRTA Team Lead. • PM.	• Acquisition Center of Excellence (ACE) • DoDI 5000.88, Engineering of Defense Systems, Section 3.5 • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix A: USAF SSE Acquisition Guidebook (1.2.1 Acquisition Strategy Panel (ASP) and 1.10 Risk Management)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
Acquisition Strategy Decision	Obtain concurrence with the MDA on strategy	If approved, proceed to WBS 2.0 to get RFP approval. If not approved, fix appropriately and go back to Acquisition Strategy.	• ASP CHART	• PM/CE	• Appendix A: USAF SSE Acquisition Guidebook (1.2.1 Acquisition Strategy Panel [ASP])
2.0	**Request for Proposal**				
2.1	**Requirements Analysis**	The Requirements Analysis Process is the method to decompose User needs (usually identified in operational terms at the system level during implementation of the Stakeholder Requirements Definition Process, see DAG Section 4.2.1) into clear, achievable, and verifiable high-level requirements. As the system design evolves, Requirements Analysis activities support allocation and derivation of requirements down to the system elements representing the lowest level of the design. Formal Cyber Survivability requirements allocation for subsystem and box-level specifications are derived by performing an SRA. Various types of SVPP analyses and tests will be performed in support of the SRA. Fundamental to the SRA are the result of trade studies and threat system interaction analyses. This sub-topical area contains information on the Requirements Analysis Process found in the DAG Chapter 3, Section 4.2.2. Generate requirements to mitigate risks and establish protections of CPI, SCF, and MCF.	• Requirements Analysis	• SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specifications, 2.3 SOO and SOW) • MIL-HDBK-520 • DAG Chapter 3 Section 4.2
2.1.1	Finalize Contractor Requirements	Utilizing WBS 1.2, WBS 1.3, and WBS 1.7, finalize contractor requirements (i.e., SOO/SOW to include CDRLs and DIDs). Ensure requirements are included for necessary test support Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP.	• SOO/SOW or equivalent	• SSWG	• DoDI 5000.89 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW)
2.1.2	Finalize System Requirements	Utilizing WBS 1.2, WBS 1.3, and WBS 1.7, finalize system requirements (e.g., SRD/Spec). Allocated Survivability requirements are formally documented (as applicable) in the system and/or segment specifications (Type A specifications), development specifications (Type B specifications), box and/or product specifications (Type C specifications), process specifications (Type D specifications) and material specifications (Type E specifications) Ensure requirements are testable, achievable, and measurable. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP.	• SRD/Spec or equivalent	• SSWG	• DoDI 5000.89 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specifications)
2.1.3	Alternative Systems Review (ASR)	Conduct ASR, if applicable, per Appendix A: USAF SSE Acquisition Guidebook Section 4.0.	• ASR Meeting minutes	• PM • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.1 Alternate Systems Review (ASR) or Engineering & Manufacturing Development (EMD) Contract Award)
2.2	**Develop Request for Proposal**	**NOTE:** Recommend having an independent review team assess the RFP for applicability and gaps prior to approval.			
2.2.1	Develop SETR SSE Entry/Exit Criteria	It is a best practice that SETR entrance and exit criteria should be included in the Integrated Master Plan (IMP) in the contract.	• IMP	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1 SETR/IMP)
2.2.2	Select DFARS AFFARS, FAR Clauses	Ensure appropriate clauses are on contract. Contact the contracting officer.	• RFP and Contract	• SSWG • Contracting officer	• DoDI 5000.02 • Appendix A: USAF SSE Acquisition Guidebook (3.1 Request for Proposal (RFP) - Contract Clauses)
2.2.3	Develop Sections L and M Criteria	Section L provides instructions to the Offeror to prepare their proposal. Section M defines Measures of Merit, which includes the factors, sub factors, and elements used to “grade” the Offeror’s proposal.	• Sections L and M	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (3.2 RFP - Section L, 3.3 RFP - Section M)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
2.3	**Programmatic Plans**	Develop/Finalize Information Support Plan (ISP), Life Cycle Sustainment Plan (LCSP), Systems Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP). Ensure SSE considerations are documented appropriately.	• SEP • TEMP • ISP • LCSP	• SSWG • ITT • CyWG	• DoDI 5000.02 • DoDI 5000.85 • DoDI 5000.88 • DoDI 5000.89 • DoDI 8500.01 • DoD Mission Engineering Guidebook, November 2020 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (1.7 Information Support Plan (ISP), 1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP)) • DoD TEMP Guidebook
2.4	**Risk Assessment**	Update SSE risks in the program's Risk Management Process and System Safety Process. Update SSE Requirements Implementation Assessment. Obtain approval from the appropriate approving authority (e.g. PM, PEO, SAE, or Chief Information Officer (CIO)). If risk assessment is not approved, return to previous steps necessary to appropriately mitigate the unapproved risks.	• Updated Risk Assessment • SSE Requirements Implementation Assessment • Hazard Assessment	• IRTA Team. • SSWG • SWG • PM • CE • System Safety Group	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix E: SSE Requirements Implementation Assessment • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • AFI 91-102_AFGM2020-01 91-202 • MIL-STD-882E • AFLCMC Standard Process for Cybersecurity Assessment and Authorization (For AFLCMC Programs) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
	Approve RFP	If approved, then proceed to WBS 3.0. If not approved, adjudicate comments appropriately.			
3.0	**Contract Award**				
3.1	**Ensure Proposal Includes Requirements & Deliverables**				
3.1.1	Establish Proposal Review Team	Ensure the proposal team has SSE representation. Appoint an SSE Sub-Factor Chief under the SE Factor Chief with evaluators from the SSWG.		• Source Selection Evaluation Board Chair • SSE • SSWG	• See Acquisition Center of Excellence (ACE) for more information
3.1.2	Proposal Review	During source selection and proposal review, ensure proposal meets requirements & deliverables from WBS 2.2. If applicable, evaluate basis of estimates for appropriate costing.	• Contract • SRD	• PM • Contracts • SSWG	• See ACE for more information
Contract Award		If contract is awarded, proceed to WBS 4.0. If contract not awarded, the PM will coordinate with the MDA for next steps.			
4.0	**Program Execution, Program Reviews & Technical Reviews**				
4.1	**Update/Align Program Protection Artifacts**				
4.1.1	Update Systems Security Working Group (SSWG) to include contractor	Update and expand the SSWG membership, roles, and charter to include the contractor team. Reference WBS 1.1 **NOTE:** CyWG membership should also be expanded to include any newly identified participating cyber test agencies.	• Updated Charter • Program Protection Implementation Plan (PPIP)	• PM • SSWG • CyWG	

WBS	Activity	Description	Artifact	OPR/ Supplier	References
4.1.2	CPI Horizontal Identification & Protection	Use CPI identification subject matter experts and technologists, security classification guidance, and DoD policy (e.g., DoDI S-5230.28). Consult the Acquisition Security Database (ASDB) and the DoD CPI HPG, including the list of example CPI, to help identify the same or similar CPI associated with other programs. For more information about the ASDB, please contact your DoD Component ASDB representative or email OSD.ASDBHelpdesk@mail.mil ASDB available via SIPRNet at https://www.dodtechipedia.smil.mil/ASDB **NOTE:** Work with the USAF Anti-Tamper Service Lead early and often for guidance.	• PPP Section 4.0, ATP	• SSWG	• DoDI 5000.83 • DoDI 5200.39 • DoDD 5200.47E • DAG Chapter 8 • DoD Critical Program Information (CPI) Horizontal Protection Guidance, v2.0 • ASDB • Appendix B: USAF Combined Process Guide for CPI and CC Identification • AT Technical Implementation Guide (TIG)
4.1.3	Update Security Classification Guide (SCG) and DD254	Update SCG and DD254 (e.g., security clearance requirements, physical security requirements for safeguarding information (SCIF, SAPF, Open storage facilities, SIPRNet terminals, storage containers) and the potential for additional security features (restricted areas/gates/guns/guards)). Reference WBS 1.2.11.	• PPP Section 5.3.6 & Table 5.3.6-1 • SOW • DD Form 254	• SSWG	• DAG Chapter 9 • DoDM 5200.01, Vol. 1 • DoDI 5220.22, CH-2 • AFI 31-101 (restricted access) • AFI 63-101/20-101 • DoDI 5200.48
4.1.4	Update Programmatic Plans	Update documents in WBS 2.3, if required.	• SEP • TEMP • ISP • LCSP	• SSWG • ITT • CyWG	• DoDI 5000.02 • DoDI 5000.82 • DoDI 5000.85 • DoDI 8500.01 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (1.7 Information Support Plan (ISP), 1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP)) • DoD TEMP Guidebook
4.2	**Conduct SSE through SE**	Conduct Program Reviews/Milestone Reviews & Technical Reviews through integrated lifecycle management with access to tech data/info needed to make risk-based informed decisions. Ensure program protection activities and system design are on track.	• PPP • LCSP • SEP	• PM • CE • SSWG	• DoDI 5000.02 • DoDI 5000.83 • DoDI 5000.88 • AFI 63-101/20-101 • DAG Chapter 3 • Appendix A: USAF SSE Acquisition Guidebook (4.1 Systems Engineering Technical Reviews (SETRs) and Integrated Master Plan (IMP)) • Appendix A: USAF SSE Acquisition Guidebook (1.11 Systems Engineering Plan (SEP)) • Appendix E: SSE Requirements Implementation Assessment
4.2.1	System Requirements Review (SRR)	Conduct SRR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the top-level system / performance requirements are adequate to support further requirements analysis, architecture, design, and test activities. In addition, verify the requirements adequately address the Cybersecurity and Cyber Resiliency requirements. Obtain Defense Intelligence Agency – Threat Assessment Center (DIA-TAC) reports for known critical components and evaluate risk to determine proper design. Complete/update the Functional Thread Analysis per Appendix C: Functional Thread Analysis, and the Attack Path Analysis per	• SRR Meeting minutes and Action Items • SVPP • DIA-TAC reports • SSE Requirements Implementation Assessment	• PM • CE • SWG • SSWG • CyWG	• DoDI 5000.02 • DoDI 5000.88 • DoD Mission Engineering Guidebook, November 2020 • AFI 99-103 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.2 System Requirements Review (SRR)) • Appendix E: SSE Requirements Implementation Assessment • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Appendix D: Attack Path Analysis. Based on findings, add/modify requirements. **Prerequisite:** Complete Requirements Analysis in WBS 2.1. If applicable, update requirements analysis in support of SRR.			
4.2.2	Develop Architecture Design	The Architecture Design Process is a trade and synthesis method to allow the Program Manager and Systems Engineer to translate the outputs of the Stakeholder Requirements Definition and Requirements Analysis processes into alternative design solutions and establishes the architectural design of candidate solutions that may be found in a system model. The Architecture Design Process, combined with Stakeholder Requirements Definition and Requirements Analysis, provides key insights into technical risks early in the acquisition life cycle, allowing for early development of mitigation strategies. This sub-topical area contains information on the Architecture Design Process found in the DAG Chapter 3, Section 4.2.3. Architecture Design Process. Identify system security related system elements and corresponding boundaries/ interconnects/interfaces. Design the architecture's boundaries/interconnects/ interfaces to be cyber secure and resilient. Attempt to identify requirements which will remediate (i.e., design out) weaknesses/vulnerabilities identified during the SSE risk assessment process. Complete a traceability of the architecture to the requirements.	• Architecture Requirements (DoDAF Views)	• SSWG	• DAG Chapter 3, Section 4.2.3. Architecture Design Process • NIST 800-160, Vol. 2 • DoDI 5000.02
4.2.3	System Functional Review (SFR)	Conduct SFR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the Functional Baseline (requirements and verification methods) are established and under formal configuration control. System functions in the system performance specification are decomposed and defined in specification for lower level elements (system segments and major subsystems). Verify the requirements adequately address the Cybersecurity and Cyber Resiliency requirements. In addition, ensure verifiable test requirements are documented. Update system boundaries from WBS 1.2.4. Functional Thread Analysis completed for SCFs, MCFs, and CPI. Submit DIA-TAC reports for known critical components and evaluate risk to determine proper design.	• SFR Meeting minutes and Action Items • DIA-TAC reports • Updated Risk Assessment • Updated Functional Thread Analysis Report • SSE Requirements Implementation Assessment	• PM, • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.3 System Functional Review (SFR)) • Appendix E: SSE Requirements Implementation Assessment • IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.4	Design / Requirements Decomposition	Complete a decomposition of the architecture and Cybersecurity and Cyber Resiliency requirements to ensure all MCF, SCF, and Functions associated with CPI are allocated. This decomposition is based on risk to obtain a cyber-secure and cyber resilient system.	• System / Subsystem requirements and architecture	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (Section 2.2 and Attachment 1) • NIST 800-160, Vol. 2 • DoDI 5000.02 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.5	Preliminary Design Review (PDR)	Conduct PDR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the Allocated baseline is established and the design provides sufficient confidence to proceed with detailed design. In addition, verify the design adequately addresses the Cybersecurity and Cyber Resiliency requirements.	• PDR Meeting minutes and Action Items • DIA-TAC reports • Functional Thread Analysis • Updated Risk Assessment • Attack Path Analysis	• PM • CE • SSWG • SWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD), 4.1.4 Preliminary Design Review (PDR) • Appendix C: Functional Thread Analysis • DoDI 5000.02 • Appendix D: Attack Path Analysis • Appendix E: SSE Requirements Implementation Assessment

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Complete an attack path analysis per Appendix D: Attack Path Analysis, ensuring boundaries are evaluated. Based on findings, add/modify requirements based on their risk re-assessments, and adjust the test strategy and plans to reflect these new requirements and their design vulnerabilities. Obtain agreement on the security requirements from the AO, TSN, USAF AT Lead, and IP. **NOTE:** PDR for Space and Missile System Center (SMC) programs could have the same detail as both PDR and CDR listed in this document, due to the unique lifecycle of space systems. Submit DIA-TAC reports for known critical components and evaluate risk to determine proper design.	• SSE Requirements Implementation Assessment • SVPP		• IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase-2)
4.2.6	Finalize Design / Requirements	Finalize the architecture, Cybersecurity, and Cyber Resiliency requirements allocation for all MCFs, SCFs, and functions associated with CPI. This decomposition/ allocation is based on risk to obtain a cyber-secure and resilient system.	• Final System / Subsystem requirements and architecture	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, and Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • NIST 800-160, Vol. 2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.7	Critical Design Review (CDR)	Conduct CDR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the product baseline is stable and the initial product baseline is established. Verify the design embodies the requirements and adequately satisfies the Cybersecurity and Cyber Resiliency requirements. Update the attack path analysis per Appendix D: Attack Path Analysis, ensuring boundaries and identified potential vulnerabilities are evaluated. Also, ensure that the information flow through actual architecture components has been identified. Based on findings, add/modify requirements and adjust cyber test strategy/scope. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP. Final Functional Thread Analysis completed for SCFs, MCFs, and CPI. Submit any remaining DIA-TAC reports and evaluate risk to determine proper design.	• CDR Meeting minutes and Action Items • DIA-TAC reports • Final Functional Thread Analysis • Updated Attack Path Analysis • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment • SVPP	• PM • CE • SSWG • SWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.5 Critical Design Review (CDR)) • Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, and Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • Appendix C: Functional Thread Analysis. • Appendix D: Attack Path Analysis. • Appendix E: SSE Requirements Implementation Assessment • IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • DoDI 5000.02
4.2.8	Test Readiness Review (TRR)	Conduct TRR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Component and system testing (i.e., Phase 3 Cyber Vulnerability Identification testing – WBS 5.2.2.1) should be initiated as early as possible (typically in a laboratory or development environment) in order to identify deficiencies and potential vulnerabilities early enough to effect system changes prior to deployment. Verify the test plans, procedures, and verification methods will adequately satisfy the test and system verification requirements. Specifically, verify the cyber test plan will test the potential cyber vulnerabilities identified during the Attack Path Analysis (or at least the high priority potential vulnerabilities). TRRs should be conducted prior to "For Score" testing for Laboratory, Ground and Flight. In	• TRR Meeting minutes and Action Items • Updated Risk Assessment • Test Plans and Procedures • Updated SSE Requirements Implementation Assessment	• PM • CE • SSWG	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.02 • DoDI 5000.89 • AFI 99-103 • AFPD 17-1 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.6 Test Readiness Review (TRR)) • Appendix C: Functional Thread Analysis. • Appendix D: Attack Path Analysis. • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020.

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		addition, verify the configuration and any delta configurations as going through the testing phase. Finally, verify all test plans and procedures are completed prior to any test execution (Laboratory, Ground, and Flight) to ensure appropriate and sufficient testing is planned. **NOTE:** Obtain an Interim Authorization to Test (IATT) prior to testing.			
4.2.9	Functional Configuration Audit/System Verification Review (FCA/SVR)	Conduct FCA/SVR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the system design is verified to conform to the requirements through analysis, demonstration, inspection, and test. In addition, verify the configuration of all verification methods has been reviewed and understood. Review Developmental Test & Evaluation (DT&E) reports. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP. Submit DIA-TAC reports for any updated critical components and evaluate risk to determine proper design.	• FCA/SVR Meeting minutes and Action Items • DIA-TAC reports • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment • AT Plan	• PM • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, 4.1.7 Functional Configuration Audit (FCA), 4.1.8 System Verification Review (SVR) • IEEE 15288.2 • Appendix E: SSE Requirements Implementation Assessment
4.2.10	Production Readiness Review (PRR)	Conduct PRR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the manufacturing and SCRM processes can support production. Verify that the Design for Manufacturing, concerning not only data and drawings, but also their Manufacturing Bill of Materials (BOM) have not introduced AT and SCRM risks, issues or concerns; and that could affect the System-Under Design's MCFs and SCFs. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP. Update the Functional Thread Analysis and the Attack Path Analysis as necessary.	• PRR Meeting minutes and Action Items • Updated Risk Assessment • SVPP • Updated SSE Requirements Implementation Assessment • AT Plan • Parts, Materials and Processes Selection List (PMPSL) • As-Designed Parts, Materials and Processes List (ADPMPL) • As-Built Parts, Materials and Processes List (ABPMPL)	• PM • CE • SSWG • SWG • USAF Space Parts Working Group (SPWG)	• DoDI 5000.88 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.9 Physical Configuration Audit (PRR)) • Appendix E: SSE Requirements Implementation Assessment
4.2.11	Physical Configuration Audit (PCA)	Conduct PCA in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the product baseline is established as verified in the FCA/SVR. Verify the design and manufacturing documentation matches to the physical configuration. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP.	• PCA Meeting minutes and Action Items • SVPP • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment • AT Plan	• PM • CE • SSWG • SWG	• IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.10 Physical Configuration Audit (PCA)) • Appendix E: SSE Requirements Implementation Assessment
4.3	**Update Program Protection Analysis and Programmatic Plans**	Reassess and update program protection analysis. This process is iterative and must be revisited again and throughout the life cycle of the program, to include: prior to each acquisition milestone; prior to each system's engineering technical review; throughout operations and sustainment; and specifically during software/hardware technology updates.	• PPP, Section 2.2, Table 2.2-1, Section 3.0, Section 4.0 and Appendix C (Criticality Analysis)	• SSWG	• DoDI 5000.02 • DoDI 5000.83 • DoDI 5000.88 • DoDI 5000.39 • DoDI 5000.44 • DoDI 8510.01 • DoDI 8500.01 • AFMAN 14-401

WBS	Activity	Description	Artifact	OPR/ Supplier	References
					- DoD Trusted Systems and Networks (TSN) Analysis - Appendix B: USAF Combined Process Guide for CPI and CC Identification
4.3.1	Develop/Update Plan of Action and Milestones (POA&M)	Develop/Update POA&M as required. Develop design remediations to reduce the probability or consequence of vulnerability exploitation. If unable to design out the vulnerability, develop and select mitigation options to limit the impact of vulnerability exploitation.	- POA&M - Security Plan	- PM/SCA	- NIST SP800-37
4.3.2	Update PPP and Applicable Appendices	Conduct appropriate information analysis in order to identify, understand, and protect the information about the program that will require classification, handling, and marking considerations. **NOTE:** It is recommended to update the Program Protection Plan for each SETR, and as often, as required after the updated analyses have been conducted to support submission at milestone decisions.	- PPP Appendices A (SCG), C (Criticality Analysis), D (Anti-Tamper Plan), E (Cybersecurity Strategy)	- SSWG	- DoDI 5200.48 - DoDM 5200.01, Vol. 1 - Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems - Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW, Attachment 2 CDRL 54) - Appendix C: Functional Thread Analysis. - Appendix D: Attack Path Analysis. - (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
4.3.3	Monitor Protection Activities	Monitor CPI and CC throughout the life cycle of the program. Monitoring includes determining if an event has occurred that requires the program to reassess CPI or its associated protections. Events may include, but are not limited to, the following: - *Operational Environment*: A change in the physical location of the system with CPI other than that for which it was originally designed. - *Protection Effectiveness:* A change in the ability of the CPI protections to deter, delay, detect, and respond to attempts to compromise CPI (e.g., presumed effectiveness of system requirements invalidated through cyber test). - *Security Classification*: A change to a relevant SCG, and thus the classification thresholds. - *System Modification*: A change to the system architecture and/or designs. - *Capability Maturation*: A change in the state-of-the-art for a particular capability and thus the thresholds used for CPI identification. - *Cyber Test Strategy*: A change in the cyber test and evaluation strategy.	- SEP - TEMP - LCSP - PPP, Section 2.2, Table 2.2-1, Section 3.0, and Section 4.0	- SSWG - PM - CE - CyWG	- DoDI 5200.39, CH-3 - AFPAM 63-113 - DAG Chapter 9 - Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP)) - Appendix B: USAF Combined Process Guide for CPI and CC Identification - Appendix C: Functional Thread Analysis - Appendix D: Attack Path Analysis - DoD Program Protection Plan Outline & Guidance
4.3.4	Update Programmatic Plans	Update SEP, TEMP, and LCSP as needed.	- SEP - TEMP - LCSP	- SSWG - PM - CE - CyWG	- DoDI 5200.39, CH-3 - AFPAM 63-113 - DAG Chapter 9 - Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP))
4.4	**Risk Assessment**	Update SSE risks in the Program's Risk Management Process and System Safety Process. In addition, incorporate risks from test reports.	- Updated Risk Assessment - SSE Requirements	- SSWG - PM - CE	- Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) - Appendix E: SSE Requirements Implementation Assessment

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Update SSE Requirements Implementation Assessment. Obtain approval from the appropriate approving authority (e.g. PM, PEO, SAE, or Chief Information Officer (CIO)) If risk assessment is not approved, return to previous steps necessary to appropriately mitigate the unapproved risks.	Implementation Assessment • Hazard Assessment • MBCRA Report • SWG	• System Safety Group	• ISO 17666:2016, Space Systems – Risk Management, 1st ed. • AFI91-202_AFGM2021-01 • MIL-STD-882 • AFLCMC Standard Process for Cybersecurity Assessment and Authorization (For AFLCMC Programs) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
4.5	**Review/Approve PPP**	The PPP will be submitted for MDA approval at each milestone review, beginning with Milestone A. **NOTE:** Program Management, to include program planning and execution, is vested in the Program Management chain of command	• PPP	• SSWG • PM • MDA • PEO	• DoDI 5000.02 • DoDI 5000.83 • AFI 63-101/20-101 • AFPAM 63-113 • DAG Chapter 9 • OSD PPP Outline and Guidance, PPP example, and OSD Evaluation Criteria
	Milestone Decision/ Decision Point	The Acquisition Strategy will define the criteria for the Milestone Decisions and Decision Points (e.g., PDR, CDR, TRR). The “Milestone Decision / Decision Point” after WBS 4.5 leads to the next program phase, as well as, verification/validation. At this point, the program should reevaluate the acquisition strategy, ensure appropriate expertise is included in the Systems Security Working Group, and continue progressing through the process again.	• Milestone Decision/ Decision Point • Updated ASP	• MDA	• DoDI 5000.02 • DoDI 5000.85 • Appendix A: USAF SSE Acquisition Guidebook (1.2 Acquisition Strategy)
5.0	**Verification / Validation**				
5.1	**Interim Authorization to Test (IATT) / Authorization to Operate (ATO)**	Assemble and submit the Security Authorization Package to receive ATO or IATT	• IATT • ATO	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW, and Attachment 2 – Contract Data Requirements Lists (CDRLs) Associated with SSE) • AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • DoDI 8510.01
5.1.1	Submit Authorization Package	Assemble the Security Authorization Package for Cybersecurity, review it with the Security Controls Assessor (SCA), and submit package for approval.	• Security Authorization Package	• SSE • SSWG • PM	• AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • DoDI 8510.01
5.1.2	Risk Acceptance (Authorization)	The AO weighs the operational need against the overall risk of operation of the system and determines if the risk is acceptable. **NOTE:** The AO may issue conditions along with the authorization decision. These authorization conditions must be met for the authorization to remain valid. **NOTE:** The AO may also determine immediate remediation is required prior to issuing an authorization decision.	• Signed Authorization (IATT/ATO)	• AO	• NIST SP800-37 • AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • DoDI 8510.01
5.2	**Developmental Test and Evaluation (DT&E) /Operational Test and Evaluation (OT&E)**				
5.2.1	Review Cyber Test Planning Artifacts	Ensure MBCRA reflects most recent system updates and test results. Review the test planning artifacts from CDR, TRR, and FCA. (WBS 4.2.7, WBS 4.2.8, and WBS 4.2.9). Update test	• Updated test plans, TEMP	• SSWG • CyWG	• USC Title 10, § 133a, 133b • Appendix C: Functional Thread Analysis

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		plans, as necessary. Ensure test plan(s) match the test strategy outlined in the CS and TEMP. Review the FTA and APA for any required changes and their resultant risks as associated with the MBCRA results.			• Appendix D: Attack Path Analysis. • DoDD 5000.01 • DoDI 5000.89 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook
5.2.2	Conduct Cyber DT&E	Conduct DT&E to verify SSE requirements and to provide knowledge to measure progress, identify problems, to characterize system capabilities and limitations, and manage technical and programmatic risks. DT&E results are used as exit criteria to ensure adequate progress prior to investment commitments or initiation of phases of the program.	• Updated Risk Assessment • Cooperative Vulnerability Identification (CVI) test report(s) • Updated cyber test portions of CS and TEMP • Vulnerability Reports • ACD test report(s) • DT&E artifacts	• SSWG • CyWG • cyber test agency	• DoDI 5000.02 • USC Title 10, § 133a, 133b • DoDD 5000.01 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 3 and 4)
5.2.2.1	Cooperative Vulnerability Identification (CVI)	Conduct CVI activities (Phase 3 cyber T&E activities) in a lab / developmental test environment. This testing and analysis is performed to identify cyber vulnerabilities early in the development / test process to effect system design (to include supporting and providing feedback to the Critical Design Review (CDR) if not already conducted), to inform follow-on Adversarial Cybersecurity Developmental Test and Evaluation (ACD), Cooperative Vulnerability and Penetration Assessment (CVPA), and Adversarial Assessment (AA) cyber test activities, and to help inform the Operational Test Readiness Review (OTRR). Test and verify system controls, Cybersecurity functionality, Cybersecurity posture, and validate earlier cyber vulnerabilities analysis through penetration testing. The CVI process includes detailed test planning and execution of vulnerability, controls, system misuse/abuse, and penetration testing based upon MBCRA and CVI activities conducted to date. Update requirements as necessary. **NOTE:** CVI testing typically consists of multiple incremental test events (beginning with individual sub-components / components and increasing to end-to-end system testing) spanning the developmental test period and occasionally into operational test if system modifications occur during operational test. Whenever possible, CVI activities should begin during system development and may include integrated contractor/Government cyber test activities.	• Updated Risk Assessment • CVI test report(s) • Updated cyber test portions of CS and TEMP	• SSWG • CyWG • cyber test agency • SWG	• USC Title 10, § 133a, 133b • AFI 99-103 • AFPD 17-1 • ISO 17666:2016, Space Systems - Risk Management, 1st ed... • DoDD 5000.01 • DoDI 5000.90 • DoDI 5000.02 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 3). • DoD PM Guidebook for Integrating the Cybersecurity Risk Management Framework into System Acq Lifecycle • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
5.2.2.2	Adversarial Cybersecurity Developmental Test and Evaluation (ACD)	Conduct Adversarial Cybersecurity DT&E upon completion of the CVI activities and vulnerability remediation/mitigation implementation (ideally on the completed system). The ACD includes an evaluation of the system's Cybersecurity using realistic tactics, techniques, and procedures while in a representative operating environment. Evaluate the system's Cyber Resiliency (i.e., capability to perform its mission while subjected to and following a cyber-attack) through	• Vulnerability Report • ACD test report(s) • DT&E artifacts • Updated cyber test portions of CS and TEMP	• SSWG • CyWG • cyber test agency	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.90 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 4)

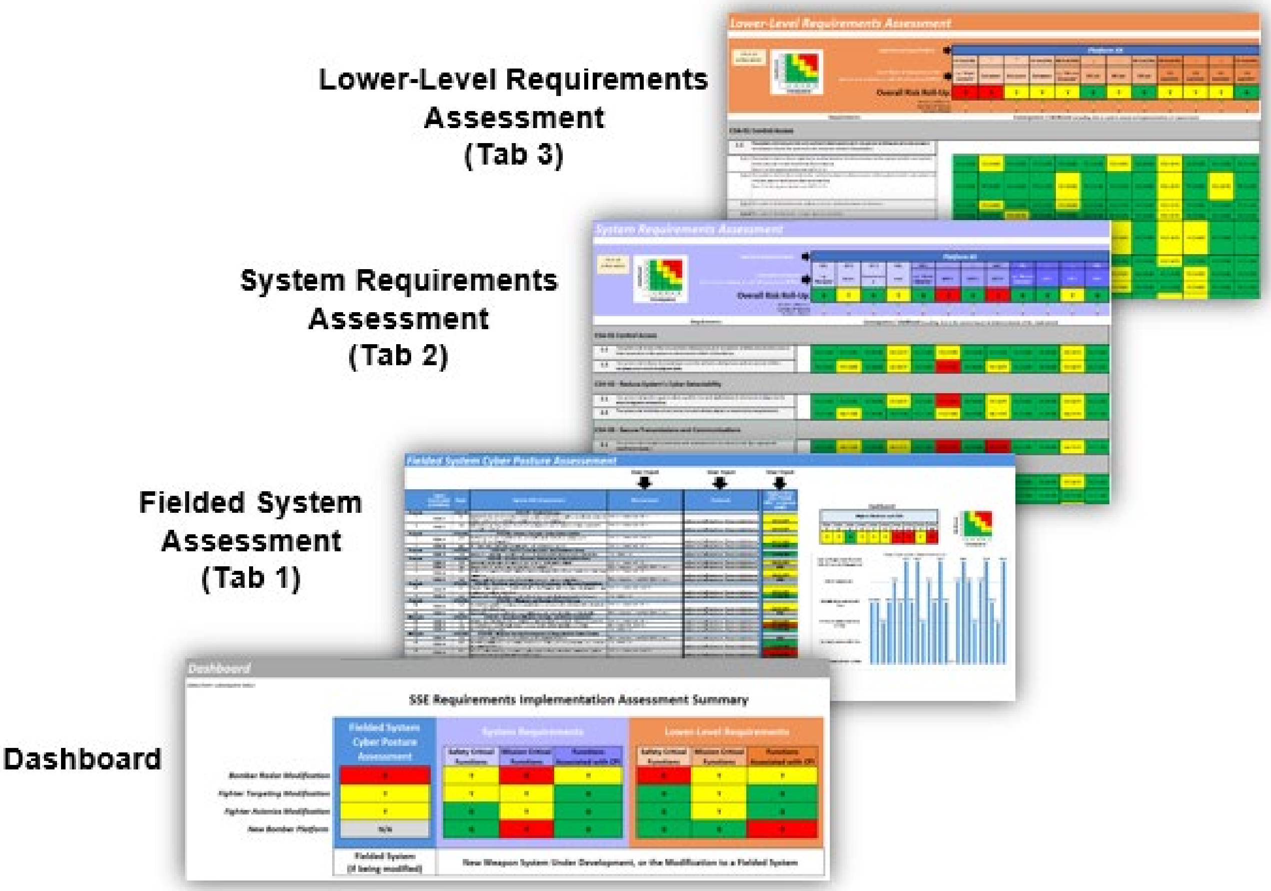
WBS	Activity	Description	Artifact	OPR/ Supplier	References
		penetration testing with the intent of causing mission effects.			
5.2.3	Conduct Cyber OT&E	Determine the operational effectiveness, operational suitability, and survivability or lethality of a system when operated under realistic operational conditions, including Joint combat operations and system-of-systems concept of employment. Evaluate whether threshold requirements in the approved requirements documents and critical operational issues have been satisfied. Assess impacts to combat operations and provide additional information on the system's operational capabilities, limitations, and deficiencies.	• Test and Evaluation Reports • CVPA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required) • Survivability and Vulnerability Program Plan (SVPP)	• SSWG • CyWG • cyber test agency • Survivability Working Group (SWG)	• DAG Chap 8, 3.2 Operational T&E • USC Title 10, § 133a, 133b • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • DoDD 5000.01 • DoDI 5000.89 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 5 and 6) • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space, 19 July 2010
5.2.3.1	Cooperative Vulnerability and Penetration Assessment (CVPA)	The purpose of the CVPA is to provide a comprehensive characterization of the Cybersecurity status of a system in a fully operational context and to substitute for reconnaissance activities in support of adversarial testing when necessary. This is an OT&E event performed by a Cyber Blue Team, which is completed either before or following MS C (as appropriate) and after the SUT has received an authority to operate or an interim authority to test in an operationally representative network(s). This testing may be integrated with DT&E activities if conducted AMCI99-101 18 JUNE 2018 11 in a realistic operational environment and in a realistic operational environment and approved in advance by the OSD Director, Operational Test and Evaluation (DOT&E). Cooperative Vulnerability and Penetration Assessment (CVPA). **NOTE:** The CVPA should be conducted after previously identified vulnerabilities are remediated or mitigated.	• Test and Evaluation Reports • CVPA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required)	• SSWG • CyWG • cyber test agency • SWG	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.89 • DoDI 5000.90 • AFI 99-103 • AFPD 17-1 • AMCI 99-101 • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • DoD Cybersecurity Test and Evaluation Guidebook (Phase 5) • DoD PM Guidebook for Integrating the Cybersecurity Risk. Management Framework into System Acq. Lifecycle • DOT&E Memo: Procedures for Operational Test & Evaluation of Cybersecurity in Acquisition Programs
5.2.3.2	Adversarial Assessment (AA)	Conduct an Adversarial Assessment following the completion of the CVPA and subsequent remediation activities. The AA assesses the capability of a unit equipped with a system to support its missions while subjected to validated and representative cyber threat activity (i.e., Cybersecurity and Cyber Resiliency testing of a system in an operationally representative environment). The OTA shall evaluate the system's capability to: • Prevent cyber intrusions from negatively impacting mission effectiveness/mission functions • Mitigate the effects of cyber-attacks, enabling the system to complete critical mission tasks • Recover from cyber-attacks and restore mission capability degraded or lost due to threat activity	• Test and Evaluation Reports • AA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required)	• SSWG • CyWG • cyber test agency • SWG	• USC Title 10, § 133a, 133bDoDD 5000.01 • DoDI 5000.90 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 6) • DoD PM Guidebook for Integrating the Cybersecurity Risk Management Framework into System Acq Lifecycle • DOT&E Memo: Procedures for Operational Test & Evaluation of Cybersecurity in Acquisition Programs • ISO 17666:2016, Space Systems – Risk Management, 1st ed.
5.3	**Generate Test Report(s)**	Capture the results of cyber DT&E and OT&E in required test report artifacts in accordance with supporting test plans. Test results will demonstrate execution of test plans, which verified and validated requirements. Upon completion of each cyber test and evaluation phase (i.e., CVI, ACD, CVPA, and AA), generate a cyber-vulnerability report.	• DT&E and OT&E reports • Updated cyber test portions of the CS and TEMP (if required)	• SSWG • CyWG	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.89 • AFI 99-103, Section 5.19, 5.20 • AFPD 17-1 • Appendix C: FTA. • DoD Cybersecurity Test and Evaluation Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Review the FTA for any required changes and their resultant risks as associated with the Test Reports results. Any identified test failures/vulnerabilities during DT&E and OT&E should be resolved by reverting to WBS 4.2 and WBS 4.4, respectively. The CyWG shares the report and all supporting documentation with SE, the Program Office, CDT, Cybersecurity testers, and stakeholder. Capture any vulnerabilities or deficiencies in Joint Deficiency Reporting System (JDRS). Deficiencies should be linked to requirements. **NOTE:** Apply Security Classification Guide to deficiency reporting.			
6.0	**Operation & Support**				
6.1	**Authorization To Operate (ATO)**	See WBS 5.1. Submit final ATO package to AO for approval, if necessary.	• ATO	• SSWG	• AFI 17-101 • DoDI 8510.01 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
6.2	**System Sustainment**	Maintain the same system security posture during the operation & sustainment phase as during the design phase. Ensure the correct DFARS clauses, security requirements, etc., are on the sustainment contract. Ensure that the Users deliver and follow an operational security plan. For any major modifications, return to the start of the WBS. For minor modifications, ensure monitoring is maintained and considered (need to follow the technical orders and have a Security Plan).	• LCSP • PPP	• Product Support Manager	• Appendix A: USAF SSE Acquisition Guidebook (3.1.2 Recommended List of DFARS Clauses)
6.3	**Monitoring**	Determine the security impact of proposed or actual changes to the system, environment, threats, and vulnerabilities.	• Plan of Actions & Milestones (POA&M) • PPP Section 9.1 & Appendix E (Cybersecurity Strategy)	• PM	• NIST SP800-37 • AFPAM 63-113 • NIST SP800-137 • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
6.3.1	Ongoing Security Assessments	Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the system in accordance with the organization-defined monitoring strategy, or at minimum annually.	• POA&M	• SCA	• DoDI 8510.01 • NIST SP800-37
6.3.2	Ongoing Remediation Actions	Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk.	• POA&M	• ISSO/ Common Control Provider	• NIST SP800-37
6.3.3	Security Status Reporting	Report changes to the risk posture of the system to the Authorizing Official in accordance with the monitoring strategy.	• PPP Section 9.0	• ISSO/ Common Control Provider	• AFI 17-101 • NIST SP800-37
6.3.4	System Removal & Decommissioning	Implement a system decommissioning strategy, when needed, which executes required actions when a system is removed from service.	• LCSP • PPP	• ISSO/ Common Control Provider	• NIST SP800-37 • Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP))
6.3.5	Program Protection Surveys	Conduct surveys on the contractor and sub-contractor facilities at least once during each integrated life cycle phase and at contract renewal.	• SOW • Performance Work Statement (PWS) • PPP Section 9.0	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.1 Performance Work Statement (PWS), 2.3 Statement of Objectives (SOO) and Statement of Work (SOW)
6.3.6	Schedule & Conduct CPI/CC Reviews	Reassess CPI and CCs throughout the life cycle of the program at least every two years throughout operations and sustainment and specifically during software/hardware technology updates.	• PPP, Section 3.0	• PM/SSWG	• DoDI 5000.39 • DoDI 5000.44 • AFI 63-101/20-101 • AFPAM 63-113

WBS	Activity	Description	Artifact	OPR/ Supplier	References
					• Appendix B: USAF Combined Process Guide for CPI and CC Identification
6.3.7	Update the PPP as Required	Review and update the PPP at minimum every five years or as threat changes.	• PPP	• SSWG	• AFI 63-101/20-101
6.3.8	Deficiency Reporting	Review Deficiency Reports (DRs) and complete root cause analysis reporting as necessary. Cyber incident response begins with the submittal of an OPREP-3B, Rule 6C report or a CCIR and includes those actions taken to respond, coordinate, analyze, and report any event or cyber Incident for the purpose of mitigating any adverse operational or technical impact. For further instructions, reference CROWS CICC IRT CONOPS, Section 7. Cyber Incident Response Process Flow. **NOTE:** Upon an incident and/or deficiency, update risk assessment.	• DR • Updated risk assessment	• SSWG • SWG	• Appendix A: USAF SSE Acquisition Guidebook (2.3.2 Program Protection) • Air Force Cyber Resiliency Office for Weapon Systems (CROWS) Cyber Incident Coordination Cell (CICC) and Cyber Incident Response Team (IRT) for Weapon Systems Concept of Operations • ISO 17666:2016, Space Systems – Risk Management, 1st ed.
6.3.9	Continuous Monitoring	Continuously monitor Cybersecurity and Cyber Resiliency activities annually, or as needed. Continuous monitoring includes the effectiveness of SSE requirements and changes to the environment for both Government and contractors.	• USAF Contractor Security Plan	• SSWG	• CDRL 19 (Appendix A: USAF SSE Acquisition Guidebook Attachment 2, and Appendix A Section 2.3.3 Cybersecurity and Trusted Systems and Networks)
6.4	**Update Risk Assessment**	Update SSE risks in the Program's Risk Management Process and System Safety Process. Obtain approval from the appropriate approving authority (e.g. PM, PEO, Service Acquisition Executive (SAE), or Chief Information Officer (CIO)). If risk assessment is not approved, return to previous steps necessary to appropriately mitigate the unapproved risks. **NOTE:** If current risks are elevated or new medium/high-risks are identified, then approval of those risks should be obtained.	• Updated risk assessment • Hazard Assessment	• SSWG • PM • CE • System Safety Group • SWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • AFI 17-101 • AFI 91-202 • MIL-STD-882 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • ISO 17666:2016, Space Systems – Risk Management, 1st ed. **Back to Workflow Process Chart**
End					

5.0. SSE REQUIREMENTS IMPLEMENTATION ASSESSMENT.

During the design and development of a new space and weapon system, or modification to an existing space and weapon system, an assessment of how Cybersecurity and Cyber Resiliency requirements are being incorporated should be performed at various steps throughout the development. Instructions for completing the SSE Requirements Implementation Assessment referenced in the WBS are contained in Appendix F. There is an accompanying Excel workbook tool in this Appendix to aid in completing the assessment (Figure 12).


Lower-Level Requirements Assessment (Tab 3)
Lower-Level Requirements Assessment
Overall Risk Roll-Up
System Requirements Assessment (Tab 2)
System Requirements Assessment
Overall Risk Roll-Up
Fielded System Assessment (Tab 1)
Fielded System Cyber Posture Assessment
Dashboard
Dashboard

SSE Requirements Implementation Assessment Summary

	Fielded System Cyber Posture Assessment	System Requirements			Lower-Level Requirements		
		Safety Critical Functions	Mission Critical Functions	Functions Associated with CPI	Safety Critical Functions	Mission Critical Functions	Functions Associated with CPI
Bomber Radar Modification	R	Y	R	Y	R	Y	Y
Fighter Targeting Modification	Y	Y	Y	G	G	Y	G
Fighter Avionics Modification	Y	G	Y	G	G	Y	G
New Bomber Platform	N/A	G	R	G	G	G	R
	Fielded System (if being modified)	New Weapon System Under Development, or the Modification to a Fielded System					

Figure 12 SSE Requirements Implementation Assessment Tool

6.0. ROLES AND RESPONSIBILITIES.

Detailed responsibilities for key Program Protection Planning tasks can be found within the WBS in Table 2, located in Section 4.5 of this document.

6.1. Program Manager.

- Conducts Program Protection Planning activities and prepares a PPP IAW this guide.
- Ensures Cybersecurity and Cyber Resiliency requirements, attributes, and design consideration are designed into newly acquired systems and modified systems.
- Ensures that the Cybersecurity Working Group (CyWG) tailors existing cybersecurity standards that reflect the analyses of specific program risks and opportunities and determine the level of cyber protections needed for their program information, the system, enabling and support systems, and information types that reside in or transit the fielded system.
- Appoints a Program Protection Lead to coordinate and execute security related tasks and facilitate the SSWG
- Ensures the PPP and annexes are reviewed and coordinated with the appropriate stakeholders.
- Submits the PPP to the MDA for approval. The PPP Appendices related to Cybersecurity and Cyber Resiliency will be coordinated and reviewed by the respective Authorizing Official (AO) or designated representatives.
- If the program is already fully deployed and there are no more milestones, the PM becomes responsible for security impacts of the change and documents them in their program's Program Protection Plan.
- Ensures that risk-reducing countermeasures for security-related threats are identified.
- Can sign the revised PPP.
- Appoints an Information System Security Manager (ISSM).

6.2. Systems Engineer

- **Ensures the development and delivery of cyber resilient capabilities through the implementation of SE balancing system cost, schedule, performance and risk assessments, based on the system's threats and vulnerabilities.**

6.3. Systems Security Engineer.

- Ensures SSE requirements are identified and included in all program documents (e.g. RFP, Statements of Work, System Specifications, etc.) including modification program documents). Refer to Appendix A: USAF SSE Acquisition Guidebook, Section 2.0 and Section 3.0.
- Ensures SSE requirements to satisfy protection needs are implemented through the SE process and tested through the program office's test program.
- Ensures security approaches are documented in the PPP.

- Ensures PPP remains current and informed by the SE reviews, constraints and decisions. Ensure emerging threats are continually assessed and incorporated in requirements/design.
- Conducts and leads program protection analyses for program and system information, CPI, and critical components.

6.4. Local Intelligence Lead.

- Ensures intelligence analysis, to include assessment of the intelligence mission data requirements, PPP objectives.
- Provides support for FTA, intelligence analysis (Intent rating), and Attack Path Exercise/Cyber War Game.

6.5. Air Force Office of Special Investigations (AFOSI).

- Collaborate with SSWG in order to produce Counterintelligence Support Plan (CISP) and periodically update it based on the updated threats to CPI and critical components.

6.6. Security Management / Information Protection (IP) (Program Protection Lead).

- Collaborate with the Systems Security Engineer in order to inform the program protection analyses and modify the security protection measures to meet program needs.
- Identify security vulnerabilities and needed security protection measures within the scope of their expertise.
- Define, implement and monitor security protection measures, and additional security requirements (i.e. awareness training, reporting, etc.).

6.7. Process Owner (Local Systems Engineering Lead).

- Reviews PPP sent up the chain to SAF/AQ and DoD.
- Maintains and coordinates changes to this process.
- Leads process improvement and change events related to this process.
- Assists Program Offices with PPP development and coordination.
- Provides training upon request.

6.8. Milestone Decision Authority/Program Executive Officer.

- Performs the roles and responsibilities established in DoDI 5000.02, DoDI 5000.85 and AFI 63-101/ 20-101.

6.9. Systems Security Working Group (SSWG).

- SSWG Lead obtains participants to include PM, Program Protection Lead (security management/information protection), Logistics, Chief Engineer, Systems Engineer, Systems Security Engineer, Information System Security Manager (ISSM), Intelligence, Defense Counterintelligence and Security Agency (DCSA), National Security Agency, and representatives from the Cyber Working Group (CyWG), AO, SWG, TSN, USAF AT Lead, and IP.
- Gathers documentation to assist with the review and understanding of what the customer requirements, capabilities, and desired effects are.
- Facilitates and ensures the completion of the Program Protection Analysis, Criticality Analysis, Initial Attack Path Analysis, Requirements Analysis and reviews results.
- Facilitates and ensures the completion of the Threat Assessment, Vulnerability Assessment, Risk Assessment and reviews results.
- Facilitates, reviews, and ensures the development of the PPP and security plans per DoDI 8500.01 and DoDI 8510.01.
- Identifies required clauses (FAR, DFARS, AFFARS) in conjunction with Procuring Contracting Officer.

6.10. Key Stakeholders (AO, TSN, USAF AT Lead, and IP).

- See WBS for responsibilities.

6.11. SSE-Portfolio Manager for CPM.

- Civilian and military co-leads responsible for the execution of capability portfolio management.
- Identifies any SSE-related enterprise services to be used (e.g., PKI certificate revocation, User attribute services, CSSPs, etc.).
- Identifies any SSE-related releasability, exportability and/or classification issues associated with web services supporting coalition, interagency, or Non-Governmental Organization (NGO) partners.

6.12. CSSP Manager.

- Maintains guidance to evaluate the maturity level of DoD Cybersecurity service providers to provide services IAW DoD O-8530.1-M.
- Develops, implements, and maintains a process to validate Federal mission partner capability to provide equivalent Cybersecurity services and evaluate the risk to the Department of Defense Information Network (DoDIN).
- Validates the designation of the systems as either SE or GENSER, as defined in the Glossary.
- Maintain a list of DoD GENSER and SE Cybersecurity service providers authorized to provide Cybersecurity services, in coordination with the CDRUSSTRATCOM; the Director, DIA; and the Director, DISA.

7.0. TOOLS AND TRAINING.

- Appendix A: USAF SSE Acquisition Guidebook.
- Appendix B: USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components Identification**.**
- Appendix C: Functional Thread Analysis
- Appendix D: Attack Path Analysis
- Centralized Cyber Capabilities Directory (C3D): **https://rdte.services.nres.navy.mil/C3D/**
- Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems: **https://www.dtic.mil/DTICOnline/home.search**
- PM Toolkit: **https://hanscomnet.hanscom.af.mil/pmtb/MR/MR.html**
- National Institute of Standards and Technology Special Publication Website: **https://www.nist.gov/publications**
- DAU iCatalog Home Page courses: **https://icatalog.dau.edu/**
- Committee on National Security Systems library of publications: **https://www.cnss.gov/CNSS/searchForm.cfm**
- E-Publishing website for Air Force instructions and publications: **https://www.e-publishing.af.mil/Product-Index/**
- For AFLCMC programs: AFLCMC Standard Process for Assessment and Authorization: **https://www.afacpo.com/apm/core-documents/reference-documents/**
- AFLCMC hosts a quarterly, 3-Day Program Protection Training class with a Distance Learning option available during the course. Course dates and links to the course can be reached here: **https://www.milsuite.mil/book/groups/acquisition-program-protection-planning**
- Defense Acquisition University offers a 12-hour ACQ 160 Program Protection Planning Awareness course available here: **https://icatalog.dau.edu/onlinecatalog/courses.aspx?crs_id=2082**
- "Product Compliant List", National Information Assurance Partnership

  https://www.niap-ccevs.org/Product/index.cfm
- USAF Evaluated Product List (EPL)

  https://usaf.dps.mil/teams/EAO/Lists/COTSGOTS%20Software/EPL.aspx

8.0. APPENDICES

Appendix A - USAF SSE Acquisition Guidebook

Guidance for incorporating SSE into programmatic documents as well as guidance for including SSE into Requests for Proposals (including tailorable requirements language). It is referenced for additional guidance throughout the main document. It will continue to be updated and released as part of this SSECG.

Appendix B – USAF CPI/CC Identification

Includes a process and guidance for identifying Critical Program Information (CPI) and Critical Components (CC). It is referenced for additional guidance on various topics in the main document. It will continue to be updated and released as part of this SSECG.

Appendix C – Functional Thread Analysis

How to perform a system functional decomposition to identify mission and safety critical functions.

Appendix D – Attack Path Analysis

Information on how to identify potential cyber-attack paths within a system.

Appendix E – SSE Requirements Implementation Assessment

A recommended, risk-based, periodic assessment during system development to verify how well the SSE requirements are being allocated against the system's critical functions.

Appendix F – Relationship to Other Processes

Mapping of the SSE Cyber Workflow Process to the DoDI 5000.02 Adaptive Acquisitive Framework pathways, DoD Cyber Test & Evaluation, and the Risk Management Framework (RMF).

Appendix G – Definitions

Appendix H – Acronym List

Appendix I – References

Appendix J – Templates

Includes the Guide's Attack Path Vignette Template and Comments Resolution Matrix (CRM) Worksheet.

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

APPENDIX A

SYSTEMS SECURITY ENGINEERING ACQUISITION GUIDEBOOK

Version 4.0

26 July 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Secretary of the Air Force, Public Affairs (SAF/PA) Case #: 2021-0424. Requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

TABLE OF CONTENTS

Table of Tables

Table of Figures

Executive Summary

This appendix provides a common starting point for Acquisition Category (ACAT) programs to develop Systems Security Engineering (SSE) content for acquisition documents. It is the intent of this guide to provide value-added, tailorable SSE acquisition language guidance that can be used across all Air Force (AF) acquisition centers. While there are a myriad of required references related to SSE, this guidebook serves to provide focus and clarity for USAF weapon and space system program offices as they protect programs by applying SSE.

Program protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. In order to manage risk, programs should apply the following countermeasures in accordance with (IAW) DoD Instruction (DoDI) 5000.02, Enclosure 3:

- Technology Readiness Assessments for Software Intensive Systems.
- Anti-counterfeit practices.
- Anti-Tamper (AT).
- Cybersecurity.
- Exportability Features.
- Hardware Assurance (HwA).
- Procurement strategies.
- Secure system design.
- Security.
- Software Assurance (SwA).
- Supply Chain Risk Management (SCRM).

SSE is an element of Systems Engineering (SE) that applies scientific and engineering principles in a standardized, repeatable, and efficient manner to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. SSE accomplishes the integrated technical management and application of methods, processes, and tools to deliver systems that satisfy stakeholder security needs for operation in contested environments.

This guidebook includes explanatory notes throughout and example language, where appropriate, to assist the Program Office (PO) in acquisition document preparation, and to facilitate the application of SSE across the acquisition life cycle. The information in this document is intended to help acquisition professionals bake-in protection capability and countermeasures (including Cybersecurity and Cyber Resiliency), and ensure it is tightly integrated into the system throughout its life cycle.

FOREWORD

"USAF Systems Security Engineering Acquisition Guidebook" introduces the latest changes in System Engineering for Defense Systems along with its SSE sub-discipline's latest Mission Engineering for space and weapon systems across the AAF lifecycle from design/modification, development and their final retirement/disposition.

Record of Changes

Version	Effective	Summary
4.0	26 July 2021	Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	Addition of Space Systems into SSE requirements assessment process.
3.0.1	29 Jan 2021	No changes to content, just updated revision numbers to correspond with body of the main document.

Document Construction.

This document uses terms such as "*SSE related*", "*SSE activity*", "*SSE considerations*", and "*SSE risk*" to refer to program protection disciplines and countermeasures including: identification of Critical Program Information (CPI), Anti-Tamper[4], Cybersecurity, exportability features, Operations Security (OPSEC), Information Security (INFOSEC), Personnel Security (PERSEC), physical security, secure system design, HwA, SwA, anti-counterfeit practices, SCRM and other mitigations IAW DoDIs 5000.02 Series, 5200.39, 5200.44, 5200.47E, 8500.01, and the Defense Acquisition Guidebook (DAG), Chapter 9. Italicized text provides the PO with language to assist in the development of well-constructed and complete acquisition documentation. The USAF SSE Acquisition Guidebook should be considered as a foundation to help acquisition professionals tailor the language as necessary to fit the characteristics of each "system" that is to be acquired for use by their programs.

NOTE: It should not be used to "cut and paste" without understanding its applicability to the program. The language in each Section may need to be modified to meet the specific needs of the PO.

To emphasize, SSE utilizes SE to integrate Cybersecurity and Cyber Resiliency requirements to achieve Cyber Survivability. The policies referenced in this document are listed in Table A-1.

Table A-1 Referenced Policies

Issuance #	Title	Description
AFI 17-101	Risk Management Framework for AF IT	This AFI provides implementation instructions for the RMF methodology for AF IT to include Platform Information Technology (PIT) (PIT systems, PIT subsystems, and PIT products).
DoDI 5000.PR	Human Systems Integration (HSI)	Establishes policy for Human Systems Integration in Defense Acquisition.
DoDI 5000.02	Operation of the Adaptive Acquisition Framework	Provide opportunities for MDAs/DAs and PMs to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired.

[4] It is strongly suggested that the reader familiarize themselves with the most current version of the Anti-Tamper (AT) Security Classification Guide (SCG) and Low Observable/Counter Low Observable (LO/CLO) SCG prior to inserting the recommended AT language into any documentation.

Issuance #	Title	Description
DoDI 5000.73	Cost Analysis Guidance and Procedures	The conduct of cost analysis to provide accurate information and realistic estimates of cost for DoD acquisition programs.
DoDI 5000.75	Business Systems Requirements and Acquisition	Establishes policy for the use of the Business Capability Acquisition Cycle (BCAC) for business systems requirements and acquisition.
DoDI 5000.81	Urgent Capability Acquisition	Establishes policy, assigns responsibilities, and provides procedures for acquisition programs that provide capabilities to fulfill urgent operational needs and other quick reaction capabilities that can be fielded in less than 2 years.
DoDI 5000.82	Acquisition of Information Technology	Establishes functional acquisition policy and procedures for all programs containing IT (including National Security Systems (NSS), excluding contractor equipment incidental to the execution of a contract.
DoDI 5000.83	Technology and Program Protection to Maintain Technological Advantage	Establishes policy, assigns responsibilities, and provides procedures for Science and Technology (S&T) managers and engineers to manage system security and Cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to DoD-sponsored research and warfare fighting capabilities.
DoDI 5000.84	Analysis of Alternatives (AoA)	Conduct physical performance AoAs for MDAPs pursuant to Section 832 of the National Defense Authorization Act for Fiscal Year 2020, and in support of the certifications to be executed pursuant to Sections 2366a and 2366b of Title 10, United States Code.
DoDI 5000.85	Major Capability Acquisition	Prescribes procedures that guide the acquisition of major capability acquisition programs, including Major Defense Acquisition Programs (MDAPs); other programs categorized as Acquisition Category (ACAT) I; major systems, usually categorized as ACAT II; Automated Information Systems (AIS) (not managed by other acquisition pathways); and other capabilities developed via the major capability acquisition pathway.
DoDI 5000.86	Acquisition Intelligence	Integration of intelligence into the acquisition life cycle.
DoDI 5000.87	Operation of the Software Acquisition Pathway	Prescribes procedures for the establishment of software acquisition pathways to provide for the efficient and effective acquisition, development, integration, and timely delivery of

Issuance #	Title	Description
		secure software in accordance with the requirements of Section 800 of Public Law 116-92.
DoDI 5000.88	Engineering of Defense Systems	Establishes policy, assigns responsibilities, and provides procedures to implement engineering of defense systems.
DoDI 5000.89	Test and Evaluation (T&E)	Establishes policy, assigns responsibilities, and provides procedures for Test and Evaluation (T&E) programs across five of the six pathways of the adaptive acquisition framework: urgent capability acquisition, Middle Tier of Acquisition (MTA), major capability acquisition, software acquisition, and Defense Business Systems (DBS). The sixth pathway, defense acquisition of services, does not require T&E policy and procedures.
DoDI 5000.90	Cybersecurity for Acquisition Decision Authorities and Program Managers	Establishes policy, assigns responsibilities, and prescribes procedures for the management of Cybersecurity risk by program decision authorities and Program Managers (PMs) in the DoD acquisition processes.
DoDI 5010.44	Intellectual Property (IP) Acquisition and Licensing	Establishes policy, assigns responsibilities, and prescribes procedures for the acquisition, licensing, and management of IP pursuant to Sections 2320, 2321, and 2322(a) of Title 10, United States Code (U.S.C.).
DoDD 5105.84	Director (Cost Assessment and Program Evaluation)	Provides acquisition support on matters relating to cost analysis, Analysis of Alternatives (AoA), and analytic competency.
DoDI 8500.01	Cybersecurity	Ensures mission risk and mission resilience are central to program and operational decisions by aligning with NIST and CNSSI Cybersecurity standards.
DoDI 8510.01	Risk Management Framework (RMF) for DoD IT	Replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle Cybersecurity risk to DoD IT.
DoDI 5200.44	“Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)”	Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components.
DoDI 5200.39	“Critical Program Information (CPI) Protection within the Department of Defense”	Counterintelligence, Security and System Engineering responsible for the identification and protection of CPI. Expands definition of CPI to include degradation of mission effectiveness.

Issuance #	Title	Description
DoDD 5200.47E	“Responsibilities for Anti-Tamper (AT) Protection of (CPI)”	Establishes policy and provides guidance for research, development (to facilitate early AT planning and design), test, evaluation, and implementation of AT.
JCIDS Manual	Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)	Establishes the System Survivability (SS) Key Performance Parameter and the key element of Cyber Survivability below it.
Public Law 114-328, SEC. 855(d)	National Defense Authorization Act for Fiscal Year 2017	Establishes mission integration activities to include joint mission areas, personnel qualifications, engineering and test responsibilities, modeling and simulation, mission-based inputs for the requirements process, and automated tools for composing Systems-of-Systems (SoS).
Security Management	Contact Center security management branch for more information	Information Security [DoDM 5200.01, AFI 16-1404], Industrial Security [DoDI 5220.22, AFI 16-1406], Personnel Security [DoDM. 5200.02/46, DoDM 5200.02, AFMAN 16-1405], Operation Security [DoDD 5205.02, AFI 10-201].
SMC-S-014 (2010)	AFSC Standard Survivability Program Management for Space	This revised standard incorporates The Aerospace Corporation Report TOR-2008(8583)-8164 rev A, “Survivability Program Management for Space”
White House	"Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, p.56155, 4 May 2020.	Section 4 establishes guidance for the United States Government approach to the cyber protection of space systems. Agencies are directed to work with the commercial space industry and other non-government space operators, consistent with these principles and with applicable law, to further define best practices, establish Cybersecurity-informed norms, and promote improved Cybersecurity behaviors throughout the Nation’s industrial base for space systems.
White House	National Space Traffic Management Policy", Federal Register, Vol. 83, No. 120, Space Policy Directive 3, p. 28969, 21 June 2018.	Set priorities for Space Situational Awareness (SSA) and STM innovation in Science and Technology (S&T), incorporate national security considerations (including the encryption of satellite command and control links and data protection measures for ground site operations), encourage growth of the U.S. commercial space sector, establish an updated STM architecture, and promote space safety standards and best practices across the international community.

1.0. Programmatic Documents

This guidebook provides a common starting point for programs to develop Systems Security Engineering (SSE) content for acquisition documents. It is the intent of this guide to provide value-added, tailorable SSE acquisition guidance for all AF acquisition centers, including the AF Life Cycle Management Center (AFLCMC), AF Nuclear Weapons Center (AFNWC), and Space and Missile Systems Center (SMC). Not all Contract Data Requirements List (CDRL) or Statement of Objective (SOO) / Statement of Work (SOW) requirements should be included in every contract. The information in this document is intended to help acquisition professionals' bake-in protection capabilities and countermeasures, including Cybersecurity and Cyber Resiliency, and ensure it is tightly integrated into the system throughout its life.

The documents in this Section are developed by the PO to ensure secure development, design, implementation, testing, and sustainment throughout each system acquisition. These documents are based on statutory and regulatory requirements at each milestone and other decision points during the acquisition process.

Since each acquisition document has a specific purpose, there is no "one-size-fits-all" SSE language. However, there are important SSE precepts to consider when a PO is preparing these documents:

- Understand the purpose of each acquisition document and tailor SSE-related language as appropriate.
- Include system security engineers as part of the upfront document development process. This ensures that the SSE-related requirements, resources, schedules, and costs are factored in early in the program.
- Ensure SSE is considered as an integral part of all programmatic activities, specifically in the areas of:
    - SE, architecture, design, development, and integration responsibilities;
    - Software engineering, architecture, open standards, design, development, integration, and software maintenance;
    - Governance, risk management, and oversight;
    - Contracting strategy and contract management;
    - Foreign Military Sales (FMS) and export controls;
    - Independent verification, validation, testing, evaluation, auditing, assessment, inspection, and monitoring;
    - System administration, operations, maintenance, manufacturing, sustainment, logistics, and support; and
    - Acquisition, budgeting, and project management.

1.1. IS-ICD and IS-CDD

Key Performance Parameter (KPP) related requirements generation is described within the Joint Capabilities Integration and Development System (JCIDS), and includes the identification of required capabilities, KPPs, Key System Attributes (KSAs), and additional performance attributes, which are included in the IS-ICD, IS-CDD, Concept of Operations (CONOPS), Information Support Plan (ISP), and Test and Evaluation Master Plan (TEMP).

As an integral part of the JCIDS process, the PO interacts with the User community to inform the development of space and weapon system requirements, including those that account for SSE activities throughout the acquisition life cycle. When drafting the IS-ICD or IS-CDD, recommendations from the Wing and Program Office must take into account SSE-related capabilities.

1.1.1. IS-ICD/IS-CDD –SS KPP / Cyber Survivability Considerations

The SS KPP is intended to ensure the system maintains its critical capabilities under applicable threat environments, to include the cyber threat. The SS KPP is applicable to all IS-CDDs, IAW the JCIDS Manual. Additional guidance on the SS KPP is provided in Enclosure D, Appendix C of the JCIDS Manual. Refer to the System Requirements Document (SRD) and System Specifications Section of this guidebook for deriving specifications from the User’s IS-ICD/IS-CDD.

The Joint Chiefs of Staff (JCS) developed the Cyber Survivability Endorsement (CSE) process through coordination across the DoD, Services, Intelligence Community (IC), and T&E community with the intent to improve Cybersecurity requirements within the IS-ICD and IS-CDD. The CSE Implementation Guide (CSEIG) helps sponsors articulate Cyber Survivability requirements with the level of granularity appropriate for use in these JCIDS documents. For more information on the CSEIG, visit:

https://intelshare.intelink.gov/sites/cybersurvivability/

The SS KPP is composed of three pillars: Prevent, Mitigate, & Recover:

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

Cybersecurity and Cyber Resiliency comprising Cyber Survivability are the results of these three pillars.

Additionally, each pillar has associated Cyber Survivability Attributes (CSAs) (Table A-2) that must be considered for incorporation into all capability requirement documents.

Table A-1 Cyber Survivability Attributes.

CSA	Pillar	Cyber Survivability Attribute (CSA)
CSA 01	*Prevent*	Control Access
CSA 02	*Prevent*	Reduce System's Cyber Detectability
CSA 03	*Prevent*	Secure Transmissions and Communications
CSA 04	*Prevent*	Protect System's Information from Exploitation
CSA 05	*Prevent*	Partition and Ensure Critical Functions at Mission Completion Performance Levels
CSA 06	*Prevent*	Minimize and Harden Cyber Attack Surfaces
CSA 07	*Mitigate*	Baseline & Monitor Systems, & Detect Anomalies
CSA 08	*Mitigate*	Manage System Performance if Degraded by Cyber Events
CSA 09	*Recover*	Recover System Capabilities
CSA 10	*Prevent* *Mitigate* *Recover*	Actively Manage System's Configuration to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP)

The CSEIG includes a process to determine the strength of CSA for the IS-ICD and IS-CDD. Refer to the CSEIG for more details. It assumes that weapons systems are considered “Very High” with respect to the Cyber Survivability Risk Category (CSRC).

1.1.2. JCS CSEIG Recommended Cyber Survivability IS-ICD Language

The following is an EXAMPLE of IS-ICD language from the CSEIG. In many cases, this can be used directly for the IS-ICDs and AoAs.

The Mission’s criticality and impact of system compromise requires that the system must survive and operate in a cyber-contested environment against the span of anticipated adversaries and threat actors that range from amateurs and unorganized cyber criminals (includes lower threat tier capabilities) to the most sophisticated, persistent, and extremely well-resourced adversaries at an advanced nation state level, capable of the highest level of cyber tradecraft that can exploit known and unknown vulnerabilities, as well as, develop and deploy sophisticated, stealthy implants. The capability must include sufficient resiliency to complete the mission in the event of cyber-attacks and effects by the anticipated adversaries. This capability’s survivability must include mitigations for Confidentiality, Integrity and Availability (C, I & A) compromises of internal and external information flows. Recognizing the adversaries’ current and projected cyber threat capabilities and cyber-attack tactics, techniques and procedures, the system must leverage available DoD cyber protections, to include consideration of protections inherited from the capability’s technologies and, as needed, build specific custom protections, countermeasures, and technologies. These protections should include at a minimum, a defense-in-depth architecture considering the inherited protections. Cyber Survivability Attributes, which *must be assessed for each alternative identified by AoA and tailored for system-specific architectures are:*

- Prevent cyber-attack effects: control access; reduce cyber detectability; secure transmissions and communications; protect information from exploitation; partition and ensure critical functions at mission completion performance levels; minimize and harden cyber-attack surfaces; and actively manage system's configuration to counter vulnerabilities at tactically relevant speeds.

- Mitigate the effects of cyber-attacks: baseline and monitor systems and detect anomalies; manage system performance if degraded by cyber events; and actively manage system's configuration to counter vulnerabilities at tactically relevant speeds.

- Recover from cyber-attacks: recover system capabilities and actively manage system's configuration to counter vulnerabilities at tactically relevant speeds.

These cyber protections and countermeasures must be identified, implemented, maintained, and patched to protect the capability throughout the system's life cycle.

1.1.3. JCS CSEIG Recommended Cyber Survivability IS-ICD Statements

- Capability to continue essential mission functions despite adverse conditions.

- Capability to track current operational state and restore mission functions after adverse conditions are detected, and change mission functions to minimize future adverse activities.

- Capability to provide an operational view of the networked environment that will provide Situational Awareness (SA) of potential threats, vulnerabilities, attacks, networks, systems, services, and other critical information to support decision-making and prevent, stop, isolate, or remediate degradation of provided services.

- Capability to enable and protect the flow of critical information to include the capability to exchange information with mission partners.

- Capability to ensure that required data, services, and information capabilities necessary to support critical warfighting functions are still available in a degraded cyber environment, to include the ability to respond to unauthorized activities.

- Capability to provide agility to rapidly assess and respond to a dynamic Cybersecurity environment.

- Capability to provide well-trained and highly proficient personnel with the knowledge, skills, and abilities required to perform day-to-day activities needed to deliver world-class Cybersecurity services.

- Capability to survive and operate in a cyber-contested environment against the span of anticipated adversaries and threat actors that range from common criminals to resourced adversaries at a nation state level, capable and willing to exploit known cyber vulnerabilities.

1.1.4. JCS CSEIG Recommended Cyber Survivability IS-CDD Language

The expectation for the IS-CDD is identifying and tailoring the 10 CSAs for system-specific implementation and updated threats to the systems. In addition, the CSA must be testable and measurable in the operational environment for Developmental Test and Evaluation (DT&E) in support of system verification of derived Cyber Survivability requirements and operational assessments of Cyber Survivability capability requirements.

Below is an example of tailored IS-CDD Language to Address CSA 6 - Minimize and Harden Attack Surfaces:

- *The <Insert SYSTEM NAME> must minimize available attack surface (access points, interfaces, ports, and removable media) to those areas hardened against attack and also necessary for mission accomplishment (Threshold). Rationale/Reference: In order to increase system survivability, the system should be more defensible. The number of access points (and opportunities for control failure) throughout the system's architecture should be minimized (e.g., interfaces, partitions, and functions). The remaining access points should be cyber-hardened to be resistant to attack.*

1.1.5. JCS CSEIG Recommended Cyber Survivability Attribute IS-CDD Language

The Cyber Survivability Risk Category (CSRC) is a system-unique attribute determined within the CSE process that integrates mission type, adversary threat tier, system cyber dependence, and Committee on National Security Systems Instruction No. 1253 impact levels. Once determined, the program office applies the CSRC to Cyber Survivability Attributes to render metrics and testable Threshold and Objective Cyber requirements. The system’s CSRC value provides program managers an objective view of cyber survivability within the context of the system’s projected mission.

The following is recommended language for the creation of system attributes to implement the CSAs. The following language assumes that the space and weapon system is considered “Very High” with respect to the CSRC. If the associated space and weapon system is not considered a “Very High” CSRC, the CSAs should be tailored, as applicable. Each attribute below should be addressed and converted to KSAs or other system attributes.

CSA 01 - Control Access.

- The system ensures that only identified, authorized, and approved persons and non-person entities are allowed access or interconnection to the system or sub-elements within its boundaries.
- Tailgating and Access Cards are good examples for ground stations.

CSA 02 - Reduce System's Cyber Detectability.

- Wireless and wired signaling and communications should not enable an adversary to target or monitor a system through its emanations or exploit the content or characteristics of such emanations.
- The system should be protected at a required cyber defense posture level (strength of cyber defense capability).

- Wireless and wired signaling and communications should not compromise OPSEC. Countermeasures must maintain the system's mission effectiveness against the anticipated levels of adversary attacks.

CSA 03 - Secure Transmissions and Communications.

- Transmission Security (TRANSEC) and Communication Security (COMSEC) protections must be implemented commensurate with the need for C, I, & A of the communications and information.

CSA 04 - Protect System's Information from Exploitation.

- The system defends against adversary attempts to exploit information resident in the system, as well as, information about the system, by unauthorized actors (to include authorized Users exceeding their privileges). This includes attempts to compromise the system's identity and access control countermeasures, or otherwise elicit information during unauthorized interactions with the system (wireless or wired).
- The system counters attempted malicious data injection, other corruption, or denial of service activities. In conjunction with vulnerability management, this includes mitigation of attacks (e.g., active scanning, script injections, etc.), which seek to identify and exploit attack vectors.
- The system also protects information at rest against corruption, exploitation, or exfiltration, as appropriate.

CSA 05 - Partition & Ensure Critical Functions at Mission Completion Performance Levels.

- The system's more critical functions and privileges should be partitioned (isolated from less critical functions) to reduce risk. Compromises of less critical functions should not prevent mission completion.
- The system mitigates effects of cyber events and any resulting system degradation by ensuring and/or recovering mission critical and supporting platform functions to a level sufficient to complete the mission.
- For required Wartime Reserve Modes (WARM), the system preserves minimum essential performance for these modes and missions.

CSA 06 - Minimize and Harden Cyber Attack Surfaces.

- In order to increase system survivability, the system should be more defensible. The number of access points (and opportunities for control failure) throughout the system's architecture should be minimized (e.g., interfaces, partitions, and functions).
- The strength of the protection for interfaces, access points, and functions should be commensurate with the system, interfaces, and mission function criticality.

CSA 07 - Baseline & Monitor Systems and Detect Anomalies.

- The system monitors the configuration baseline for cyber anomalies (e.g. leaks, intrusions, and attack effects) in critical functions, components, or information support, and provides "risk posture status" (i.e., SA). The timeliness for identification of the anomalies must support timely response to the anomaly's effects to minimize damage, and preserve minimum essential functions needed for mission completion.

- When necessary, the system includes automated responses that facilitate operator intervention to sustain functions; or support operator activities (man-in-the-middle) for prioritization and response to cyber events; and as needed, support recovery to a trusted operational condition.

CSA 08 - Manage System Performance if Degraded by Cyber Events.

- When degraded by cyber events, the system maintains minimum performance required from the system before unacceptable mission consequences occur.
- The system avoids sudden, unrecoverable, or catastrophic failures, and enables mitigations of cyber-attack effects through orderly, structured, and prioritized system responses (which may be invoked based upon the first indicator of cyber-attack, e.g., immediately shed lower priority functions, preserve/conserve/safeguard resources, and further reduce the cyber-attack surface).
- The system continues to perform mission critical functions, including essential platform support, in spite of cyber-attacks, degraded communications services, or information leakage.

CSA 09 - Recover System Capabilities.

- The system, depending upon the mission criticality, and cyber event effects, should be able to recover mission critical functions in near real-time to continue its mission (fight through the attack).
- The system, and all of its subsystems, components, and information support, can be returned to a fully operational state, after the effects of a cyber-event and newly discovered cyber threats have been mitigated (hardware and software recovery to fight another day).

CSA 10 - Actively manage system configurations to achieve and maintain an operationally-relevant Cyber Survivability Risk Posture (CSRP)

- The system must be maintained to preserve its Cyber Survivability capabilities through appropriate vulnerability management including, but not limited to patch management, mitigation of known threats, and effects of obsolescence, which impacts cyber survivability.
- The system's vulnerability management must evolve to address changes in threat, in CONOPS, and in intended operational environment.

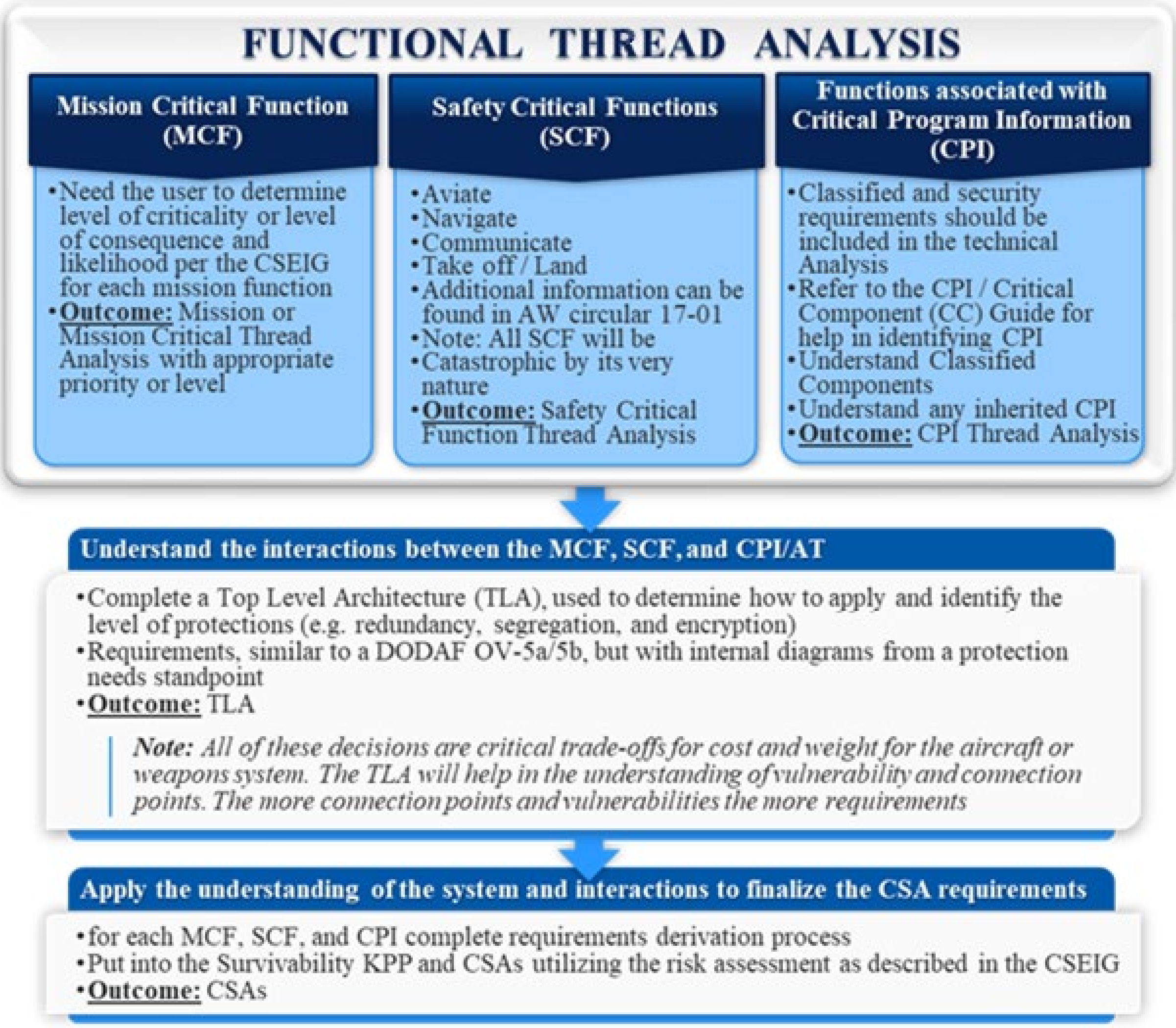
1.1.6. High-Performance Team (HPT) Implementation of Survivability KPP & CSAs

AFI 10-601 states, “The purpose of the HPT is to provide the appropriate level of consistent cross-functional involvement in requirements generation from IS-ICD to IS-CDD to produce executable, risk-based, fiscally informed requirements that deliver affordable capabilities at optimal cycle time to the warfighter.”

After the HPT execution to establish the IS-ICDs and/or IS-CDDs for the Survivability KPP and CSAs and distributed through the Requirements Approving Authority (RAA), the SSWG’s and SWG’s roles should follow the Functional Thread Analysis process / methodology in Figure A-1 to ensure the requirements are allocated appropriately. In the case of Space Systems, refer to the SVPP for the threat environments and their effects on mission and system survivability. It is important to ask the MAJCOMs what the most critical missions and/or mission critical functions are. This is especially true with multi-mission platforms like in the Tanker platforms (e.g., Tankers typically have three types of missions: 1) Aerial Refueling, 2) Aeromedical, and 3) passenger/cargo). These steps will help the programs complete the Functional Thread Analysis to identify mission critical functions, safety critical functions, and functions associated with CPI. For more information on CPI, refer to **Appendix B: USAF Process Guide for CPI and Critical Component Identification**.

The criticality is defined by the Cyber Survivability Endorsement Implementation Guide and risk per Section 1.10 of this Appendix. The criticality analysis provides the PO with the information needed to derive requirements to implement each of the JCIDS CSAs, and provides the basis for requirements traceability from the capabilities defined in the IS-ICD/IS-CDD to the detail design requirements documented in the **System Requirements Document (SRD) and System Specifications (SS)**. For more information on the Functional Thread Analysis, see **Appendix C**.

The JCIDS documentation uses the term Cyber Survivability. This Guidebook uses the terms Cybersecurity and Cyber Resiliency. Cyber Survivability is the overarching term for both Cybersecurity and Cyber Resiliency. Additionally, the ten CSAs are categorized as one or more pillars (Prevent, Mitigate, and Recover) which align and support achieving overall Cyber Survivability (i.e. Cybersecurity and Cyber Resiliency). The requirements derived from the 10 CSAs will satisfy all SSE current policies and those required for the SRR. It is important to understand that Cyber Survivability cannot be obtained or maintained without Cybersecurity and Cyber Resiliency.



FUNCTIONAL THREAD ANALYSIS

Mission Critical Function (MCF)

- Need the user to determine level of criticality or level of consequence and likelihood per the CSEIG for each mission function
- **Outcome:** Mission or Mission Critical Thread Analysis with appropriate priority or level

Safety Critical Functions (SCF)

- Aviate
- Navigate
- Communicate
- Take off / Land
- Additional information can be found in AW circular 17-01
- Note: All SCF will be
- Catastrophic by its very nature
- **Outcome:** Safety Critical Function Thread Analysis

Functions associated with Critical Program Information (CPI)

- Classified and security requirements should be included in the technical Analysis
- Refer to the CPI / Critical Component (CC) Guide for help in identifying CPI
- Understand Classified Components
- Understand any inherited CPI
- **Outcome:** CPI Thread Analysis

Understand the interactions between the MCF, SCF, and CPI/AT

- Complete a Top Level Architecture (TLA), used to determine how to apply and identify the level of protections (e.g. redundancy, segregation, and encryption)
- Requirements, similar to a DODAF OV-5a/5b, but with internal diagrams from a protection needs standpoint
- **Outcome:** TLA

> ***Note:*** *All of these decisions are critical trade-offs for cost and weight for the aircraft or weapons system. The TLA will help in the understanding of vulnerability and connection points. The more connection points and vulnerabilities the more requirements*

Apply the understanding of the system and interactions to finalize the CSA requirements

- for each MCF, SCF, and CPI complete requirements derivation process
- Put into the Survivability KPP and CSAs utilizing the risk assessment as described in the CSEIG
- **Outcome:** CSAs

Figure A- 1 CSA Requirements Allocation

Cyber Resiliency is defined as, “The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.” Another way to visualize Cyber Survivability is in the form of a pyramid. Cybersecurity serves as the foundation to which Cyber Resiliency can build upon to complete the pyramid. Without the foundation (Cybersecurity - like encryption, ensuring software is secure, etc.), the pyramid cannot be complete, and Cyber Resiliency cannot be obtained and maintained, as depicted on Figure A-2.

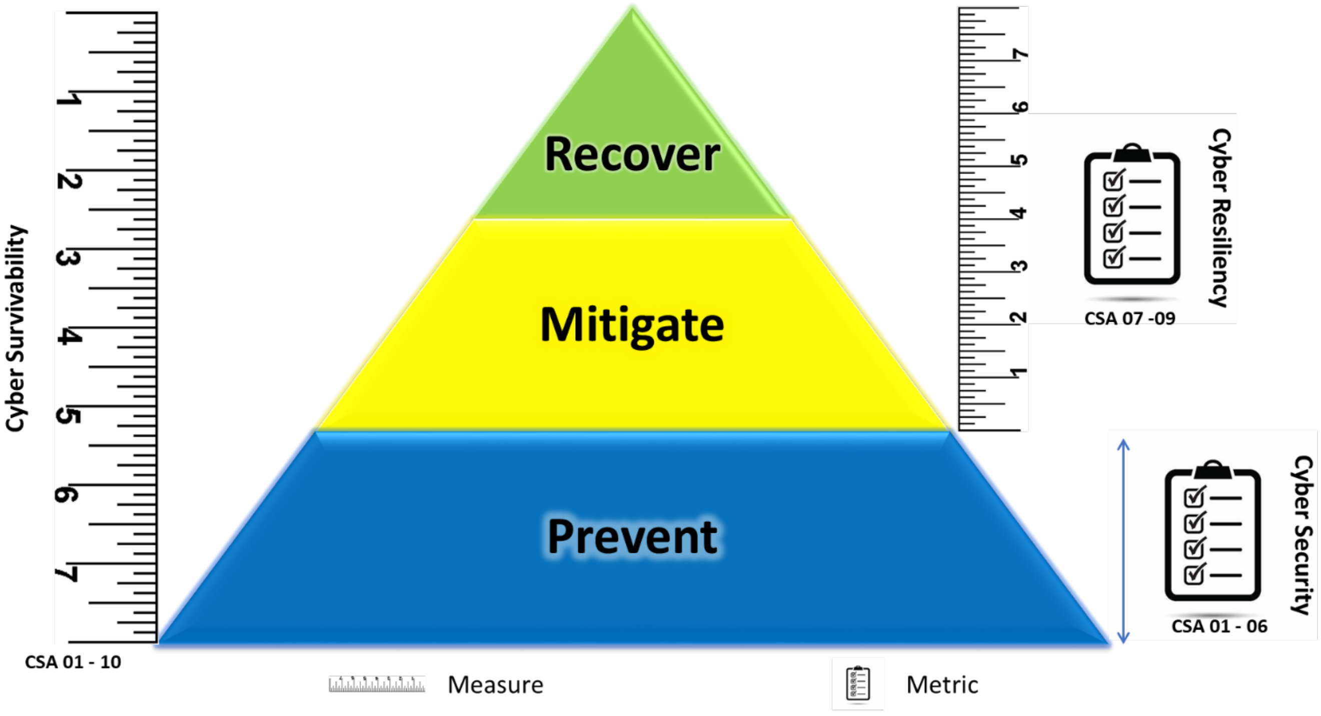


Figure A-2 Cyber Survivability Pyramid[5]

It is important to note that Cybersecurity alone does not guarantee Cyber Resiliency or Cyber Survivability. Cyber Resiliency demands measures in degrees of success in preserving the system-under-investigation's technical and operational performance. Those measures are often expressed in Technical Specification Requirements derived from the requirements documents, military and Government standards, the inherent system design limitations, and system's mission capability needs.

Baking-In" Cyber Resiliency is heavily dependent on the architectural choices at the mission and system levels. At the mission level, a robustly designed mission architecture, verified and validated through cyber mission thread analysis, is the principal means for achieving Cyber Resiliency. The emphasis at this level is on mission concepts of operation and interactions among systems. At the system level, cyber resiliency arises out of a number of attributes. One attribute is to stipulate in designs that any safety- or mission-critical function be provided by more than one subsystem such that no single cyber vector of attack could simultaneously degrade the functionality of all of the subsystems that provide that SCF or MCF, a property we call Cyber Survivability.

[5] "Cyber Survivability Endorsement Implementation Guide", Version 2.0, Joint Chiefs of Staff, Table 1, p. 17, 12 March 2020.

1.2. Acquisition Strategy

The Acquisition Strategy (AS)[6] is developed by the Program Office (PO) and is a comprehensive plan that describes the acquisition approach to managing program risks and meeting program objectives. An approved AS will inform development of the final Request for Proposal (RFP) for the next phase of a program. The Program Manager (PM) ensures the AS is consistent with SSE and program protection guidance. If applicable, include SSE considerations in the following AS Section(s):

- Section 2, "Capability Need," Subsection 2.3 – Summarize the threat assessment in relation to the capabilities or operational concepts the system must support (see the applicable System Threat Assessment Report (STAR) and/or Validated Online Lifecycle Threat (VOLT) document for details). Specify which elements of the threat (if any) are not yet fully defined, and which elements of the threat (if any) are not currently being countered by the system capabilities or Concept of Operations (CONOPS). Include a projected plan/schedule to define and counter the remaining threat elements.

- Section 3, "Acquisition Approach" – Include any SSE-related considerations contributing to unique program circumstances (i.e., transition to Defensive Cyber Operations (DCO) provider, cloud computing services, etc.) and/or new capabilities, existing system modifications or system replacements (i.e., enhanced Cybersecurity capabilities, crypto modernization, etc.).

- Section 4, "Tailoring," Subsection 4.2 – Include any SSE-related waiver requests that impact the AS (i.e., Clinger Cohen Act (CCA), etc.).

- Section 5, "Program Schedule," – Include any key SSE-related milestones and interdependencies that impact the AS (i.e., Cybersecurity assessments, multiple Authorizing Officials (AOs), Interconnection Security Agreements (ISAs), National Security Agency (NSA) cryptographic certifications, etc.).

- Section 6, "Risk and Risk Management," – Identify any SSE-related risks and summarize mitigation plans, including key risk-reduction events. List and assess any SSE-related interdependency issues that could impact execution of the AS.

- Section 7.4, "Sustainment Strategy," Subsection 7.4.3 – Provide an overview of the sustainment-related contract(s) including efforts to ensure secure and integrated information systems across industry and Government that enable comprehensive SSE risk mitigations.

[6] See **AFI 63-101, Para 4.3 for additional details.** PEOs may have additional requirements. Review PEO-specific guidance for details.

- Section 7.5, “Major Contract(s) Planned,” Subsection 7.5 – Include any major SSE-related contracting and subcontracting activities that identify the purpose, type, value, performance period, and deliverables of the contract (i.e. Third party SwA, Cybersecurity service providers (CSSPs), etc.). Specify how SSE-related testing and processes, including life cycle management and sustainability requirements, have been incorporated into the contract. Identify the SSE activities stated in the RFP and required of the contractor to demonstrate achievement of design requirements. Include any key SSE-related source selection evaluation considerations and criteria. Identify any planned use of SSE-related Government-furnished special test equipment, unique tooling, or other similar contractual requirements (e.g., National Cyber Ranges, other specialized SwA, firmware, AT, SCRM, spectrum testing, or cryptographic testing).

- Section 7.6, “Technical Data Rights Strategy,”

    - Subsection 7.6.2 – Provide an analysis of data needs to implement the product support life cycle strategy, which includes SSE considerations. Strategy should also address data rights related to SSE and what, if any, data rights are maintained by the contractor.

    - Subsection 7.6.3 – Describe approach for use of open system standards that have been developed and tested to meet certain levels of Cybersecurity, such as Open Mission Systems (OMS)/Universal Command and Control Interface (UCI) and Future Airborne Capability Environment (FACE).

- Section 8, “Cost and Funding,” – Ensure SSE-related life cycle costs and funding requirements are included in overall funding profile, shortfalls, funding charts and cost control plans.

- Section 9, “Resource Manning,” – Ensure SSE-related resources are included in manning profiles.

- Section 10.3, “Foreign Military Sales,” – Specify the potential or plans for foreign military and/or Direct Commercial Sale (DCS), and the impact upon program cost due to program protection and exportability features. Identify export quantities per fiscal year and per unit cost savings by year, resulting from export quantities.

1.2.1. Acquisition Strategy Panel

The Acquisition Strategy Panel (ASP) consists of a standing panel of senior advisors that are responsible for reviewing the proposed acquisition strategy in order to ensure that all significant considerations associated with a system acquisition have been addressed, including Cybersecurity and Cyber Resiliency. The ASP should take place as early as possible in the acquisition planning, and the ASP briefing itself should include a description of how Cybersecurity and Cyber Resiliency considerations are incorporated into the acquisition strategy. The following is the recommended Cybersecurity and Cyber Resiliency chart to include in the technical portion of the ASP briefing:

- Has the program completed a Criticality Analysis (CA) to inform the system level requirements and system design architecture, based on risk?

- Has the appropriate authority agreed per the different tenets below? Who and When?

Per DoDD 5000.01, Program Managers will employ SSE practices and prepare a Program Protection Plan (PPP) to guide their efforts and the actions of others to manage the program risks to Mission Critical Functions (MCFs), Safety Critical Functions (SCFs), and functions associated with Critical Program Information (CPI). The System Security Engineer (SSE) shall populate the ASP chart, and the PM, Director of Engineering (DoE), and Chief Engineer (CE) shall approve the content of this Cybersecurity and Cyber Resiliency ASP chart. Once the content of the chart is approved, the slide is presented as a part of the Acquisition Strategy Panel, at which time the PO provides the “sufficiency assessment” (see Section 4.0 examples below).

The content below provides high-level guidance for filling out the chart:

- The first column (“Authority and Date Concurrence”) is included to ensure that the applicable authorities are in agreement with the strategy for addressing given technical areas. The column should be populated with the name of the authority and the date that they concurred with the approach (e.g., for Critical Program Information/AT, the USAF AT Lead’s name and date would be annotated).

- The program needs to annotate, in the notes Section of the power point, the documentation/artifact(s) with the signatures of the agreement for the Criticality Analysis by the different authorities.

NOTE: Criticality Analysis should be based on MCFs, SCFs, and functions associated with CPI.

Table A-2 Cybersecurity and Cyber Resiliency ASP Chart

Cybersecurity and Resiliency	Authority and Date of Concurrence	SRD / SSS	Statement of Objectives (SOO) / Statement of Work (SOW) / Performance Work Statement (PWS)	Request for Proposal (RFP) Section L / Section M	FAR / DFARS / AFFARS Clauses	Sufficiency Assessment
Program Protection			***Ex: Section 2.3***			***Ex: G***
Cybersecurity (to include Trusted Systems and Networks [TSN])						
Critical Program Information /Anti-Tamper (AT)						
Security Management						
Cyber Resiliency						

The program will fill out the Table appropriately with a reference to the location of the Section in the Request for Proposal (RFP). If the RFP does not require Cybersecurity and Cyber Resiliency requirements, then place "n/a" in the ASP Chart. For more information, regarding the appropriate content for the items identified in the first row of the Table, please reference the following Sections of this document:

- **Performance Work Statement (PWS).**
- **System Requirements Document (SRD) and System Specifications.**
- **Statement of Objectives (SOO) and Statement of Work (SOW).**
- **Request for Proposal (RFP) – Contract Clauses.**

NOTE: The RFP Contract Clauses contain the recommended lists of FAR, DFARS, and AFFARS Clauses.

- **Request for Proposal (RFP) – Section L.**
- **Request for Proposal (RFP) – Section M.**

Due to the RFP's level of maturity, some Sections of the Table may not be able to be filled out. In this case, place "applicable" or "not applicable (n/a)" in the chart, and ensure the authorities agree with the applicability determination. As the program matures, populate the Table with the highest level of fidelity.

The PO provides a sufficiency assessment based the information provided in the ASP chart. Some examples are listed below:

- Green – The RFP package contains adequate cyber language in the RFP agreed by the proper authority per Appendix A: SSE Acquisition Guidebook
- Yellow – The Authority has not approved the RFP/Solicitation, but the program has sufficient rationale to proceed. (Put Recommend rationale in notes Section of slide).
- Red – No cyber language is in the RFP per Appendix A: SSE Acquisition Guidebook (Recommend rationale be put in notes Section of slide).

Additional applicable SSE policy and guidance: DoDI 5000.83, DoDI 5000.83, DoDI 5200.39, DoDI 5200.44, DoDD 5200.47E, DoDI 8500.01, DoDI 8510.01, and AFI 17-101.

1.3. Broad Agency Announcement (BAA)

The PO may decide to issue a BAA notice that requests scientific or research proposals from contractors concerning certain areas of interest to the Government. BAAs may be used to fulfill an organization's requirement for scientific study and experimentation directed toward advancing the state-of-the-art, or increasing knowledge/understanding rather than focusing on a specific system or hardware solution. The proposals submitted by the contractors under a BAA may eventually lead to a contract. Use of a BAA to solicit for research and development is encouraged when:

- The Government desires new and creative solutions to problem statements.
- Using a conventional SOW could result in unintentionally stifling ideas and concepts given many possible approaches.
- Fulfilling requirements for scientific study and experimentation directed toward advancing the state-of-the-art, or increasing knowledge or understanding rather than focusing on a specific system or hardware solution.
- The Government must be able to state its objectives in terms of areas of need or interest rather than specific solutions or outcomes.
- Meaningful proposals with varying technical/scientific approaches are reasonably anticipated.
- Evaluation will be based on a peer or scientific review.

Example SSE BAA Statements:

- Research is needed in the areas of theory, protocols, and techniques that will assure delivery of trustworthy data to support battlefield missions. The Government seeks novel ideas in fundamental research areas such as information-theoretic security and the science of security, which will provide direct guidance in the design of secure tactical wireless systems. In particular, topics of interest include new paradigms for physical layer security (ranging from confidentiality to authentication to trustworthiness in physical layer communications), the fundamental bounds in key management in distributed systems, the exploitation of key establishment and distribution protocols, and trusted information delivery and dissemination in mobile environments. Wherever possible, provide where the De-Identification of data and its re-identification can be achieved by different approaches, algorithms and/r tools.

- Assurance principles and metrics are needed to help define, develop, and evaluate future robust and resilient systems and network architectures that would survive sophisticated attacks and intrusions with measurable confidence. The Government seeks the capability to measure a complex system and to produce a scalar value that can determine the trustworthiness of that system.

- Current cyber defenses are often static and governed by lengthy processes, while adversaries can plan their attacks carefully over time and launch the attacks at cyber speeds at times of their choosing. The Government seeks a new class of defensive strategies to present adversaries with a moving target where the attack surface of a system keeps changing.

Space and Missile Systems Center (SMC) Recommendations

- The Government seeks new cyber testing capabilities to assess potential vulnerability to threats in the projected or actual environment of operation.
- The Government seeks new cyber testing capabilities to identify and assess vulnerabilities in a system and its environment of operation.
- The Government seeks new methods to identify, specify, design, and develop protective measures to address system vulnerabilities.
- The Government seeks new ways to identify and evaluate protective measures to ascertain their suitability, effectiveness, and degree to which they can be expected to reduce mission risk.
- The Government seeks the capability to provide assurance evidence to substantiate the trustworthiness of SSE countermeasures.
- The Government seeks the capability to identify, quantify, and evaluate the costs and benefits of protective measures to inform engineering trade-off and risk treatment decisions.
- The Government seeks the capability to leverage multiple protection-related focus areas to ensure SSE countermeasures are appropriate, effective in combination, and interact properly with other system capabilities.

1.4. Clinger Cohen Act (CCA) Compliance Report

The CCA Compliance Report verifies PO compliance with the 11 key elements identified in DoDI 5000.82 (Tables 2 and 10 and Enclosure 11) and Air Force Manual (AFMAN) 17-1402, “Air Force CCA Compliance Guide” 20 June 2018. Cybersecurity is key element number 9. If applicable, include SSE considerations in the following CCA Compliance Report Section(s):

- Attachment 2, “AF CCA Compliance Table Element 9” – Ensure that the program has a Cybersecurity Strategy that is consistent with DoD policies, standards, and architectures, to include relevant standards. If appropriate, identify Cybersecurity Strategy, Program Protection Plan, and Security Plan for Risk Management Framework.

The SAF/CIO A6XA CCA Point of Contact can be contacted directly or through the CCA Workflow box[7] The Defense Acquisition Guidebook https://dag.dau.mil/Pages/Default.aspx and the USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site[8] contain authoritative sources, information, and templates to aid in preparing a CCA compliance package and in learning about DoDI 5000.90 and IT acquisition.

1.5. Cost Analysis Requirements Description (CARD)

The CARD is developed by the PO and formally describes the acquisition program for purposes of preparing both the DoD component cost estimate and the independent cost assessment. If applicable, include SSE considerations in the following CARD Section(s):

- Section 1.0, “System Overview.” – Highlight any SSE-related details under System Description. List any SSE-related hardware, firmware and software identified in the Work Breakdown Structure (WBS) for the system. Include SSE protection countermeasures and embedded security under “System Configuration”. Also, describe any SSE-related Government-Furnished Equipment (GFE) and Property (GFP) (e.g., static or dynamic code analysis, use of trusted foundry, specialized test software/equipment, cryptographic equipment, etc.).

- Section 1.2, “System Characteristics.” – Describe SSE-related equipment (hardware, firmware and software). Include any subsystem equipment and identify which items are Off-The-Shelf (OTS) along with which open standards are being considered. Under “Programming Description,” address the programming language and programming support environment (including standard tools and secure programming practices) and the compiler(s) and/or assembler(s) to be used.

- Section 1.3, “System Quality Factors.” – Include any SSE-related specialized requirements to include software quality processes and the flow down of Reliability, Availability and Maintainability (RAM) requirements.

[7] **usaf.pentagon.saf-cio-a6.mbx.af-cio-clinger-cohen-compliance@mail.mil**

[8] **https://cs2.eis.af.mil/sites/10774/default.aspx**

- Section 1.4, “Embedded Security.” – Describe any potential embedded security in the system, including software, hardware, and firmware requirements (e.g., AT, cryptography, firmware, Field Programmable Gate Arrays (FPGAs), Application Specific Integrated Circuits (ASICs), etc.).

- **NOTE:** Reference the appropriate Security Classification Guide for the information provided, as details of embedded security may be classified.

- Section 2.0, “Risk.” – Include any SSE-related risks, to include both technical and programmatic based, as well as, these risks that impact system security (e.g. cost, schedule, etc.).

- Section 3.0, “System Operational Concept.” – Describe the system's physical security, INFOSEC, OPSEC features, SSE-related hardware, firmware, and software components and countermeasures.

- Section 3.4, “Logistics.” – Describe if any SSE-related protection techniques require special procedures under hardware, firmware, and software support concepts.

- Section 5.0, “System Manpower Requirements.” – Include manpower requirements for SSE, to include engineering and integration, implementing SSE requirements, and assessing countermeasures (e.g., Security Control Assessors (SCAs), Red/Blue Teams, threat assessments, counterfeit parts testing, special HwA or SwA testing, etc.) throughout the program’s life cycle.

- Section 9.0, “System Development Plan.” – Discuss any SSE-related demonstration and validation, engineering and manufacturing development, production, and operation activities and support. Include any SSE-related development and operational testing to be accomplished (e.g., Cross Domain Solution (CDS), Type-1 crypto, modified development processes, 100% software design/code inspections, functional testing, penetration testing, fuzz testing, vulnerability scans, Air Force Anti-Tamper Evaluation Team (ATET), third-party assessment, off-nominal testing, etc.).

- Section 10.0, “Element Facilities Requirements.” – Identify any SSE-related Government tools, test organizations, or facilities (e.g., National Cyber Ranges; Red/Blue Teams; other specialized HwA, SwA, firmware, AT, SCRM or cryptographic verification tools or testing; use of Trusted Foundry, etc.).

1.6. Cybersecurity Strategy

The Cybersecurity Strategy is developed by the PO and formally describes the Cybersecurity approach for the acquisition. It is a statutory requirement for mission critical or mission essential Information Technology (IT) systems and a regulatory requirement for all other programs containing IT, including National Security Systems (NSS). POs should ensure all systems and supporting networks dedicated to, and/or required for development, operation, and maintenance of the weapons system are identified in the Cybersecurity Strategy. PMs should seek to consolidate system boundaries as much as possible and allocate security controls as appropriate to the systems within those boundaries. This minimizes duplication of costly RMF packages for every system. The initial submittal of the Cybersecurity Strategy occurs at milestone (MS) A as Appendix E of the PPP. A draft update is due for the Development RFP Release (Dev RFP Rel) decision point and is approved at MS B. Updates to the Cybersecurity Strategy are required for MS C and the Full-Rate Production or Full Deployment (FRP/FD) decision. If applicable, include SSE considerations in the following Cybersecurity Strategy Section(s):

- Section I, “Introduction.” – (A) Include SSE-related concepts, methodologies, and outcomes that support the Cybersecurity Strategy. (C) Describe the system being acquired in terms of SSE concepts, such as technical performance, reliability, resilience, survivability, restoration, and sustainability of security functions and services, to include security function and service failure modes, behaviors, interactions, and outcomes.

- Section II, “Sources of Cybersecurity Requirements.” – (A) Include how SSE-related process and activities support categorization. (C) Describe the SSE-related requirements, to include Cybersecurity, as defined in the Information Security Initial Capability Document (IS-ICD) and Information Security Capability Development Document (IS-CDD) as part of the System Survivability Key Performance Parameter (KPP) and any other capability requirements defined by any other KPPs, key system attributes, or additional performance attributes. Include the applicability or non-applicability of the System Survivability KPP as it applies to SSE, Cybersecurity or Survivability in a cyber-contested environment. (D) Include any additional SSE-related requirements that affect the Cybersecurity approach and their sources (including but not limited to the Statement of Objectives (SOO)/Statement of Work (SOW), CDRLs with corresponding data item descriptions, system requirements document, and system specifications). Describe the approach for documenting the bidirectional traceability between SSE requirements and security controls.

- Section III, “Cybersecurity Approach.” – (A) Include how the SSE technical management processes support Cybersecurity stakeholder communication and documentation preparation. Describe how SSE agreement processes support the inclusion of Cybersecurity requirements in contracting activities. (B) Describe how the SSE interfaces (including Cybersecurity boundaries) are reflected in the overall system architecture. Describe how SSE technical processes support the incorporation of Cybersecurity requirements in the system design and architecture. Describe how Cybersecurity risk assessments are part of the overall programmatic and SSE risk management activities. Define the security context and boundaries of the system in terms of interfaces, interconnections, and interactions with external entities. Identify applicable Information Security Interface Control Documents (IS-ICDs). Identify the SSE milestones, to include Cybersecurity, as reflected in the program Enterprise Master Schedule (EMS) and Integrated Master Schedule (IMS). (**NOTE:** the functional thread analysis provides the information needed to populate this section).

- Section IV, "Cybersecurity Implementation." -- (A) Identify and update the SSE-related items in the Progress Summary. (B) Describe the SSE-related aspects, considerations, and characteristics associated with Cybersecurity implementation, to include the choice of implementation technology, implementation method, enabling systems, and target level of assurance. Include how implementation is accomplished by hardware fabrication; software development; adaptation and reuse of existing capabilities; the acquisition or leasing of components and services; and the development of life cycle concept policies and procedures to govern the actions of individuals in their use of and interaction with the technology/machine and physical elements of the system. Provide the security components of the DoD Architecture Framework (DoDAF) as identified in the Information Support Plan (ISP). Identify the bidirectional traceability between SSE requirements and security controls. Include any deviations from the Government's technical baseline(s). Describe how other SSE-related analyses, including Trusted Systems and Networks (TSN) analysis, have informed the implementation of Cybersecurity, including design, architecture, engineering changes, and other mitigations for the protection of critical functions. List and describe which SE and SSE-related documentation support Risk Management Framework (RMF) authorization activities. Include any key SSE-related risks, decisions, and trades that have been made as a result of programmatic SE and SSE risk assessments. Describe the SSE-related technical review entry and exit criteria (refer to SSECG Appendix A section 4.1) that have been developed and how they support and/or impact Cybersecurity. List any SSE-related criteria that were not met that impact Cybersecurity, and describe plan to address unmet criteria.

- Section V, "Risk Management." – (A) Include any significant outstanding SSE-related technical risks that impact Cybersecurity. Identify proposed solutions and/or mitigation strategies, including technical solutions and/or tactics, techniques, and procedures. Include the impact on Cybersecurity of not addressing these SSE-related risks. Include the SSE-related risk assessment that addresses cost, schedule, and performance impacts. Describe how these risks are being communicated. (**NOTE:** Refer to SSECG Appendix A sections 1.10, 2.2, and 2.3 and Appendix E).

- Section VI, "Policy and Guidance." – Include any SSE-related policy and guidance used to support the Cybersecurity Strategy.

- Section VII, "Point of Contact(s)." – Include relevant SSE-related Government and contractor points of contact (e.g., Lead SSE, Lead SwA Engineer, etc.) and stakeholders (e.g., Milestone Decision Authority (MDA), Operational Test and Evaluation (OT&E) agency, USAF AT Lead, User community, etc.).

- Section VIII, "Other Considerations." – Include any other SSE-related considerations that may impact the Cybersecurity Strategy.

1.7. Information Support Plan (ISP)

The ISP is developed by the PO and describes a system's dependencies and interface requirements to enable testing and verification of interoperability and supportability requirements. SSE considerations also need to be addressed in the ISP. Systems security engineers support security architecture development in conjunction with SE efforts to develop the overall architecture. The security architecture will demonstrate the set of physical and logical security-relevant representations (i.e., views) that conveys information about how the system is partitioned into security domains, enforces security policies within and between security domains, and how data/information and/or hardware will be protected. SSE considerations are included in the ISP in the following applicable sections:

- Introduction. – Include any SSE-relevant elements in the overview and program data (e.g., classification, releasability, exportability, Authorization to Operate (ATO) dates, etc.). Discuss any SSE-related programmatic relationships that may affect this system's development schedule or operational effectiveness.
- Program Data. – Include the DoD IT Portfolio Repository (DITPR) number, not the Information Technology Investment Portfolio System (ITIPS) number. Include the appropriate distribution statement in accordance with DoDI 5230.24. For most ISPs, this will be Distribution Statement D. Include an Export Control warning statement (when applicable) in accordance with DoDI 5230.24 and DoDD 5230.25. Be sure to include any applicable SSE-related handling, disposal, and destruction notices. Additionally, include Controlled Unclassified Information (CUI) markings when applicable in accordance with DoDI 5200.48 and the CUI Registry.
- Process Analysis. – Include all SSE-relevant internal and external nodes that interact with the program. Identify if there are any non-Radio Frequency (RF) interfaces with and/or node of an external wired/fiber digital network. Identify any SCRM-related results of the program's critical mission threads analysis and the comparison of the operational architecture views to the system architecture views to ensure all Critical Program Information (CPI)/Critical Component (CC) needs and dependencies are being met. If the PO identifies engineering (Tier 1), Cybersecurity (Tier 2), and protection (Tier 1) as applicable Joint Capability Areas (JCAs)[9], then SCRM input must be provided to this Section. Ensure SCRM key practices/requirements are captured in the approved system performance specification and traced to the JCIDS requirements. Include transport methodology (e.g., Internet Protocol (IP)-routed data, web service, Voice over Internet Protocol (VoIP), etc.); threat analysis system implementation; any metadata tagging; enterprise/web service usage; IP version 6 (IPv6) compatibility; etc. Analyze the SSE-relevant components of the

[9] **https://cs3.eis.af.mil/sites/OO-AQ-AF-18/default.aspx.**

Implementation Baseline (IB), Common Computing Environment (CCE), Joint Information Environment (JIE), Federal Data center Consolidation Initiative (FDCCI), and DoD cyber discipline implementation.

- Net-Centricity. – Describe the Information Enterprise (IE) in terms of general SSE-related policies used for sharing information, key infrastructure and services to be used, key aspects of Cybersecurity that will be addressed, and the SSE-related shared data spaces used. List the SSE-related Communities of Interest (COI) and the COI Point of Contact (POC) (name, org, email, and phone number) in which the program participates and which publish the metadata/taxonomies/vocabularies used by the program (e.g., DCO, Information Operations (IO), etc.). List any SSE-related Net-Centric Enterprise Services (NCES) core enterprise services the program utilizes (e.g., Identity and Access Management (IdAM), Public Key Infrastructure (PKI), Public Key Enabling (PKE), etc.). Identify any SSE-related authorizations (e.g., Cybersecurity, crypto, etc.) required to enter and be managed in the networks to be used for net centric data exchange, or to provide the security needed for effective information exchange.
- Capability Portfolio Management (CPM). – Identify any SSE-related enterprise services to be used (e.g., PKI certificate revocation, User attribute services, CSSPs, etc.). Identify any SSE-related releasability, exportability and/or classification issues associated with web services supporting coalition, interagency, or Non-Governmental Organization (NGO) partners.
- Cybersecurity. – Discuss the program's Cybersecurity Strategy, reference the PPP and assess compliance with DoD and AF Cybersecurity guidance. Include details concerning what steps the program is taking to both comply with Cybersecurity requirements and address Cybersecurity risks. Include how SSE-related aspects are included in the Test and Evaluation Master Plan (TEMP). Describe how SSEs have translated security controls to design requirements and integrated them into system specifications. Identify how Cybersecurity is being balanced with interoperability and supportability, per DoDI 8330.01. Provide location and approval status of the PPP and the program's Cybersecurity Strategy. If no Uniform Resource Locator (URL) exists, provide copy of approved document.
- Other Information Needs and Additional Operational Risks. – Identify any SSE-related needs, nodes, facilities, and connectivity to enable development, testing, and training (e.g., include separately funded SSE-related training or testing facilities the program intends to use).
- Radio Frequency Spectrum Needs. – Identify any SSE-related considerations and/or risks pertaining to the radio frequency spectrum needs, including TEMPEST, Electromagnetic Environmental Effects (E3) for radio frequency systems, emitters, and receivers. Provide supporting documentation and mitigation strategy for each.
- Miscellaneous Analysis. – Identify any Off-The-Shelf (OTS) software or integration services, of which includes commercial items [e.g., Commercial-Off-The-Shelf (COTS)] and Non-Developmental Items (NDI) [e.g., Government-Off-The-Shelf (GOTS)], list the OTS IT brand names, list any Free and Open

Source Software (FOSS) being used, and identify if the program is using any DoD Enterprise Software Agreements[10].

- Risks and Issues. – Include any SSE-related low, medium, and high-risks and issues identified as part of the program's development, operations, test, training, and processes.
- Appendix A, "References." – Include any SSE-related references.
- Appendix B, "System Data Exchange." – Include any SSE-relevant data exchanges.
- Appendix C, "Interface Control Agreements." – Include any SSE-relevant Interface Control Agreements (ICAs), to include Cybersecurity-related Information Security Agreements (ISAs).
- Appendix D, "Acronyms." – Include any SSE-related acronyms.
- Appendix E, "List of Attachments." – Include the program's PPP (with appropriate appendices), and any SSE-related architecture products (e.g., system security or crypto architectures, etc.).
- Appendix F, "Relationship to Other Processes." – Include the mapping of the SSE Cyber Workflow Process to the Risk Management Framework (RMF) and the Mission Based Cyber Risk Assessment (MBCRA) process.

1.8. Life-Cycle Sustainment Plan (LCSP)

The LCSP is developed by the PO and documents the sustainment strategy implementation. An initial draft of the LCSP is due at Milestone A, with updated versions due at program initiation (Milestone B) and the beginning of the Production and Deployment phase (Milestone C). The final version of the LCSP is required at the Production Readiness Review (PRR) for full-rate production. Refer to DoDI 5000.02 for more information on these delivery requirements.

Include SSE considerations in the following LCSP Section(s):

- Section 2.0, "Product Support Performance." – Include any SSE-related sustainment performance requirements, including KPPs, KSAs, APA and other requirements identified in RFPs.
- Section 3.0, "Product Support Strategy." – Identify the SSE-related mission critical subsystems resulting from the Criticality Analysis (CA) and risk mitigations to keep these subsystems operational. Ensure SSE efforts to identify and refine protection measures apply throughout the life cycle of the system, to include the patch and vulnerability management methodology and process. SSE-affected Configuration Items (CIs) must have 100% positive control and accountability at the appropriate classification level throughout the life cycle of the component and/or the component

[10] www.esi.mil

data, subsystem data, or system data (including prognostics-related system health data). Implement a real-time component tracking system for CIs containing CPI/CC requirements throughout the life cycle of the CI. Develop response-reporting procedures for CIs containing CPI/CC. To protect CPI, it may be necessary to limit the level and extent of maintenance a foreign customer may perform. This may mean maintenance involving some hardware and/or software will be accomplished only at the contractor or U.S. Government facility in the U.S. or overseas. Such maintenance restrictions may be no different from those imposed on U.S. Government Users. Contracts, purchase agreements, memoranda of understanding, memoranda of agreement, letters of agreement, or other similar documents shall state such maintenance and logistics restrictions. Maintenance instructions and Technical Orders (TOs) must clearly indicate the level at which maintenance is authorized and include warnings that state, “Damage may occur if improper or unauthorized maintenance is attempted.” Contracts, purchase agreements, Memoranda Of Understanding (MOUs), Memoranda Of Agreement (MOAs), Letters Of Agreement (LOAs), or other similar documents shall state such maintenance and logistics restrictions. When a contract that includes SCRM or AT protection requirements and associated maintenance and logistics restrictions also contains a warranty or other form of performance guarantee, the contract terms and conditions shall establish unauthorized maintenance or other unauthorized activities. Tamper investigation and reporting may require a classified annex.

- Section 3.1, “Strategy Considerations,” Subsection 3.1.1, “Obsolescence Management.” – Include SSE-related data for the management plan, known or predicted obsolete parts for all program system specifications, obsolete parts with suitable replacements, and actions to address obsolete parts without suitable replacements (e.g., parts requiring SCRM testing and certification, etc.).

- Section 3.1, “Strategy Considerations,” Subsection 3.1.3, “Property Management.” – Include SSE-relevant operating material and supplies, general equipment, and inventory of list of items to be tracked (e.g., Foreign Military Sales (FMS), Government, industry, third party, etc.).

- Section 3.1, “Strategy Considerations,” Subsection 3.1.4, “Cybersecurity.” – Include the appropriate SSE-related planning details from the PPP (to include Cybersecurity Strategy, Anti-Tamper Plan (ATP) and SCRM, etc.), and identify the PM responsible for SSE-related activities during system sustainment and disposal.

- Section 3.1, “Strategy Considerations,” Subsection 3.1.5, “Other Sustainment Considerations.” - Identify SSE-related cross-functional sustainment issues and risks that are design and/or cost drivers, especially as they impact the system's integrated product support elements [e.g., counterfeit parts management, controlled-item management (e.g., subsystems or components that are cyber critical, classified, export controlled, pilferable, and require data wiping prior to disposal), software sustainment, etc.].

- Section 3.3, “Product Support Agreements.” – Include any SSE-related contract support providers and performance agreements (e.g., specialized HwA, SwA, firmware, AT, SCRM or cryptographic verification personnel, tools or testing, etc.).

- Section 4.0, “Program Review Issues and Corrective Actions.” – Include any SSE-related sustainment issues identified during Program Management Reviews (PMRs) and technical reviews. Identify the findings, corrective action, and completion dates.

- Section 5.0, “Influencing Design and Sustainment.” – Identify SSE-related statutory, DoD and AF-level policy (regulations, issuances, manuals, instructions, etc.) requirements that affect a system’s design and performance (e.g., FY14 National Defense Authorization Act (NDAA), Section 803 impacts sustainment, is documented in the PPP and will be reviewed at each milestone). Identify any SSE-related requirement related cost-drivers for the program.

- Section 6.0, “Integrated Schedule.” – Include SSE-related events and milestones in the product support schedule. Ensure alignment with the IMS. Include major SSE-related activation activities for sites in the supply chain required to support the system, to include maintenance (e.g., field, depot, overseas, and ashore), supply, and training. Describe any SSE-related interdependencies and interactions with other space and weapon systems or System of Systems (SoS).

- Section 7.0, “Cost and Funding.” – Include SSE in the cost estimates and funding appropriation type, and year of funds. Summarize SSE-relevant funding required for each of the logistics elements identified in the LCSP (e.g., sustainment contracts, disposal, specialized test equipment, new or upgraded facilities, support equipment, training, and technical data requirements, etc.). Identify specific impacts that will result from any SSE-related budget shortfalls and where possible, tie these impacts to the system’s sustainment requirements (e.g., KPP, KSA, etc.). Refer to Section 1.5., “Cost Analysis Requirements Description (CARD)” for further details and direction.

- Section 8.0, “Management.” – Include SSE-relevant data (e.g., roles, responsibilities, authorities, products, and metrics) for all stakeholders, sustainment Integrated Product Teams (IPTs) and supporting agencies (e.g., Defense Information Systems Agency (DISA), Joint Federated Assurance Center (JFAC), etc.). Identify SSE-related sustainment risks and associated mitigation plans.

- Section 9.0, “Supportability Analysis.” – Include SSE-related sustainment and logistics components for design interfaces, supportability analysis and sustainment engineering. Describe how SSE considerations will be included in Deficiency Reports (DRs).

- Annex: Product Support Business Case Analysis. – Include SSE-related considerations.

- Annex: Independent Logistics Assessment and Corrective Action Plan. – Include SSE-related considerations.

- Annex: System Disposal Plan. – Include SSE-related considerations.

- Annex: Preservation and Storage of Unique Tooling. – Include SSE-related considerations.

- Annex: Core Logistics Analysis. – Include SSE-related considerations.

- Annex: Replaced System Sustainment Plan (RSS). – Include SSE-related considerations.

- Annex: Intellectual Property Strategy. – Include SSE-related considerations

1.9. Program Protection Plan (PPP)

The PPP and its appendices is developed by the PM and is the single source used to coordinate and integrate all protection efforts including sustainment after operational deployment. The PPP is developed and based on Deputy Assistant Secretary of Defense for Systems Engineering [DASD (SE)] "Program Protection Plan Outline & Guidance," Version 1.0, July 2011. The PPP documents the comprehensive approach to SSE analysis and the associated results. The PPP is approved by the MDA. The initial submittal of the PPP occurs at MS A. A draft PPP update is due for the Development RFP Release Decision Point and is approved by the MDA at Milestone B. Updates to the PPP are required for MS C and FRP/FD decision. The PPP may require a higher classification level based on the information included within. SSE considerations are included in the PPP Section(s) listed below:

- Section 1.2, "Program Protection Responsibilities." – Identify who is responsible for SSE efforts in Table 1.2-1: Program Protection Responsibilities (e.g., SSE Technical Lead, Cybersecurity Architect, Information Systems Security Manager (ISSM), SwA Technical Lead, SCRM Technical Lead, contractor, etc.).

- Section 2.1, "Schedule." – Include SSE deliverables, events, and milestones as an overlay to the Government's EMS.

- Section 2.2, "CPI and Critical Functions and Components Protection." – Identify countermeasures used for any CPI/CC listed in Table A-4.

- Section 5.0, "Threats, Vulnerabilities, and Countermeasures." – Summarize any identified threats and vulnerabilities to CPI/CC. Identify any SSE countermeasures selected to mitigate risks of compromise.

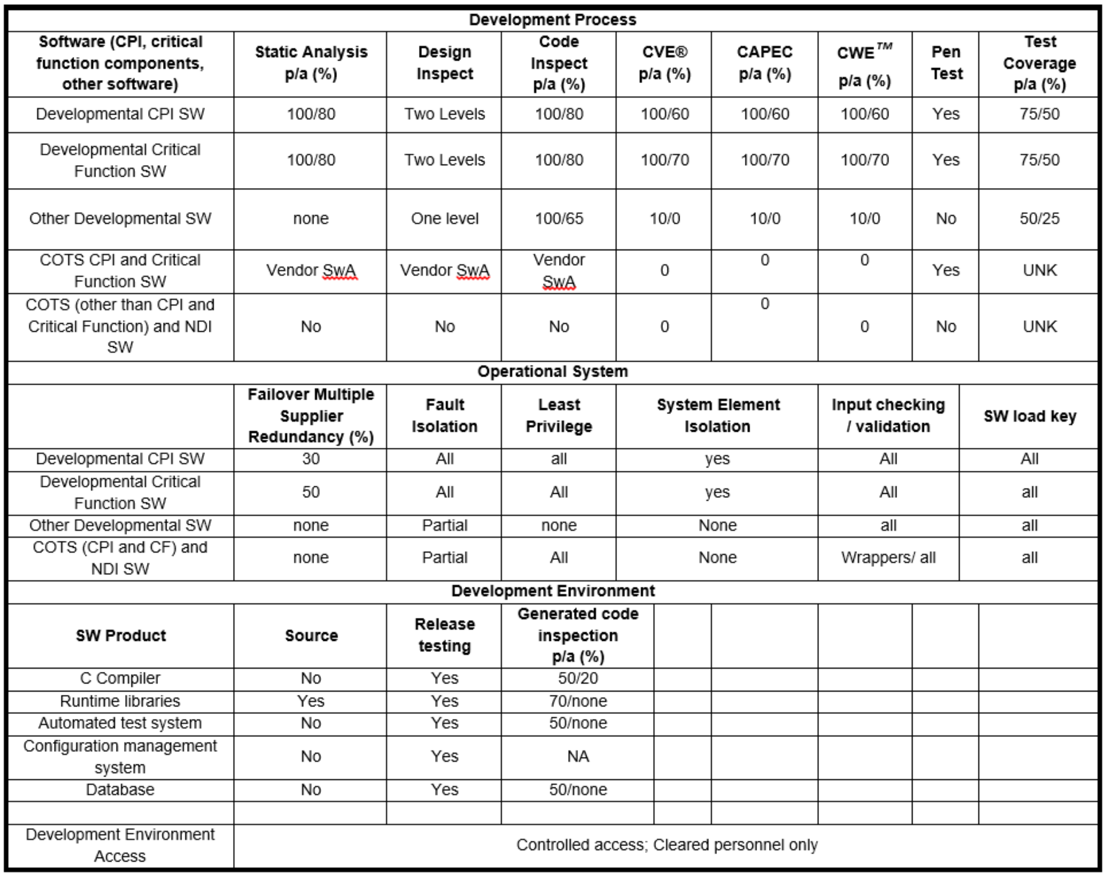
- Section 5.3, "Countermeasures." – Identify who is leading the SSE efforts. Describe the implementation of each countermeasure used to protect CPI/CC. Be specific - If SCRM key practices apply, describe which ones; if using software assurance techniques, explain which ones.

- Section 5.3.1, "Anti-Tamper (AT)." – Describe who must identify AT requirements and who is responsible for developing the ATP. Identify when the concept, initial and final ATP must be completed. Describe plans for engaging with the respective Government AT Lead and, the USAF Anti-Tamper Lead.

- Section 5.3.2, "Cybersecurity." – Describe who is responsible for assessing the adequacy of Cybersecurity countermeasures for CPI/CC and the key Cybersecurity schedule milestones; how Cybersecurity protections for CPI hosted on contractor-owned information systems (or other non-DoD information systems) are implemented; and how Cybersecurity requirements will be flowed down.

- Section 5.3.3, “Software Assurance.” – Identify who is leading the SwA efforts; describe the linkage between software assurance and the Software Development Plan (SDP) and how software assurance considerations will be addressed; how software will be designed and tested to assure protection against weaknesses; how software architectures, environments, designs, and code be evaluated with respect to Common Vulnerabilities and Exposures (CVE®), Common Attack Pattern Enumeration and Classification (CAPEC™), and Common Weakness Enumeration (CWE™); how software will be evaluated to identify unnecessary standard services, subroutines, and network protocols; how COTS/FOSS software, foreign produced software, and software of unknown pedigree (i.e. software from unknown sources and developed by unknown parties) will be protected and tested/vetted; how the development environment will be protected; and how updates (fixes) to COTS, GOTS, and FOSS software used in the system will be integrated during development and operations, etc. Update Table 5.3.3-1: Application of Software Assurance Countermeasures (sample shown in Table 1.9-1).

Table A-3 Sample Table for Application of Software Assurance Countermeasures[11]



Development Process								
Software (CPI, critical function components, other software)	**Static Analysis p/a (%)**	**Design Inspect**	**Code Inspect p/a (%)**	**CVE® p/a (%)**	**CAPEC p/a (%)**	**CWE™ p/a (%)**	**Pen Test**	**Test Coverage p/a (%)**
Developmental CPI SW	100/80	Two Levels	100/80	100/60	100/60	100/60	Yes	75/50
Developmental Critical Function SW	100/80	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25
COTS CPI and Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than CPI and Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK

Operational System						
	Failover Multiple Supplier Redundancy (%)	**Fault Isolation**	**Least Privilege**	**System Element Isolation**	**Input checking / validation**	**SW load key**
Developmental CPI SW	30	All	all	yes	All	All
Developmental Critical Function SW	50	All	All	yes	All	all
Other Developmental SW	none	Partial	none	None	all	all
COTS (CPI and CF) and NDI SW	none	Partial	All	None	Wrappers/ all	all

Development Environment								
SW Product	**Source**	**Release testing**	**Generated code inspection p/a (%)**					
C Compiler	No	Yes	50/20					
Runtime libraries	Yes	Yes	70/none					
Automated test system	No	Yes	50/none					
Configuration management system	No	Yes	NA					
Database	No	Yes	50/none					
Development Environment Access	Controlled access; Cleared personnel only							

- Section 5.3.4, “Supply Chain Risk Management.” – Describe how the program will manage supply chain risks to CPI and critical components to ensure proper hardware assurance protection per the latest PPP template and DoDI 5200.44. Explain how supply chain threat assessments will be used to influence system design, development environment, and procurement practices. Indicate if any ASICs require trusted fabrication or if the program makes use of accredited trusted suppliers of integrated circuit related services. Describe what counterfeit prevention measures will be in place and how the program will mitigate the risk of counterfeit insertion during Operations and Maintenance (O&M).

[11] (Table from Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) and DoD Chief Information Officer “*Software Assurance Countermeasures in Program Protection Planning*”, March 2014.)

- Section 5.3.5, "System Security Engineering." – Describe who in the Government is responsible for SSE; the linkage between SSE and the Systems Engineering Plan (SEP) and how system security design considerations will be addressed.

- Section 9.1, "Audit/Inspections." – Identify how the program will implement periodic SSE audits and inspections, to include those performed by independent, third-party entities (e.g., Cybersecurity Red/Blue Teams, SCAs, AF ATET, etc.).

- Section 9.2, "Engineering/Technical Reviews." – Identify how SSE will be addressed in technical reviews. Identify the SSE entry/exit criteria for these reviews.

- Section 10.0, "Processes for Monitoring and Reporting Compromises." – Define what constitutes an SSE event (e.g., Cybersecurity intrusion, malicious code discovered, crypto failure, counterfeit parts found, etc.).

- Section 11.2, "Acquisition and Systems Engineering Protection Costs." – Include any SSE-related costs in
  Table 11.2-1.

- Appendix A: Include the program's Security Classification Guide (SCG) – Ensure the **Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems** and the Anti-Tamper Security Classification Guide are applied when developing the Program SCG.

- Appendix B: Include the program's Counterintelligence Support Plan (CISP).

- Appendix C: Include the results of the program's most recent CA.

- Appendix D: Include the program's ATP.

- Appendix E: Include the program's Cybersecurity Strategy.

1.10. Risk Management

Ensure that Cybersecurity and Cyber Resiliency risks are included as an integral part of the program's risk management process and documented in the Risk Management Plan (RMP). In addition, ensure all Authorizing Officials' (AOs) and Security Control Assessors' (SCAs), Trusted Systems and Networks, Anti-Tamper/Critical Program Information, and Security Management/Information Protection risk processes are incorporated. Program Managers will report on Cybersecurity and Cyber Resiliency risks at the same time and in the same format as programmatic (cost/schedule/performance) risks.

Keep in mind that programmatic and NIST-based risk assessment scoring are based on estimates. Often, engineering risk assessments are not properly factored into the program's risk register by a proper weighting methodology used for normalizing quantitative and qualitative data within the risk register. This demands that the PO consider the use of a tool, vice hand-scoring method for collating engineering and business-related risks within the same risk register to include those risk assessments made for safety, airworthiness, and space systems.

Cybersecurity and Cyber Resiliency risks are risks to Department of Defense (DoD) warfighting capabilities from foreign intelligence collection; from malicious and inadvertent insider threats; from hardware, software, and cyber vulnerability or supply chain exploitation; and from reverse engineering due to battlefield loss or export throughout the system life cycle.

NOTE: Space systems are unique in their design and operational environment, where mission and safety critical functions require a disciplined engineering estimate vice subjective ranking/scoring system. ISO 17666:2016 defines the principles and requirements for integrated risk management on a space project. However, when the information, data and means to conduct a probabilistic or non-deterministic risk analysis for a space system are available, then ISO 17666:2016, "Space Systems – Risk Management" should be utilized for the risk assessment process.

DoDI 5000.90 delineates Cybersecurity within the supply chain by conducting several Cyber-SCRM processes to minimize any cyber threats induced from the component vendors. PMs will conduct SCRM. This includes, at a minimum, conducting market research to assess potential vendors to determine if they:

1. Provide products and components, or sub-components, sourced through original equipment manufacturers or authorized resellers

2. Have previously incurred significant malicious network intrusions, data breaches, loss of client data or intellectual property

3. Have obtained a CMMC certification level indicating that they practice, or at least, basic cyber hygiene (e.g. access management, timely patch management, identity management and password management

AFI 63-101/20-101 establishes the requirement for PMs to accomplish risk management on all programs. AFPAM 63-128 and the *DoD Risk, Issue, and Opportunity (RIO) Management Guide for Defense Acquisition Programs* provide additional risk management guidance.

Table A-5 has been derived from NIST SP800-30 r1.0, DoDI 8510.01 – *Risk Management Framework (RMF) for DoD Information Technology (IT)* and AFI 17-101 – *RMF for Air Force IT*, which contain requirements for risk management specific for IT and Platform IT systems.

Table A-4 Risk Management Process Step

Risk Management Process Step	Instructions
Risk Management Planning	AFI 63-101/20-101, AFPAM 63-128, ISO 17666:2016, ISO 11231: 2019, DoD RIO Guide, and additional considerations from this guidance.
Risk Identification	This document
Risk Assessment - Likelihood	DoDI 5000.90, Cybersecurity for Acquisition DA & PMs, Table 1, "SCRM Actions by Risk Tolerance Level," p 14, 31 December 2020
Risk Assessment - Consequence	DoDI 5000.90, Cybersecurity for Acquisition DA & PMs, Table 1, "SCRM Actions by Risk Tolerance Level," p 14, 31 December 2020
Risk Assessment - Risk	DoDI 5000.90, Cybersecurity for Acquisition DA & PMs, Table 1, "SCRM Actions by Risk Tolerance Level," p 14, 31 December 2020, ISO 17666:2016, ISO 11231:2019
Risk Handling Planning & Implementation	AFI 63-101/20-101, AFPAM 63-128, and DoD RIO Guide, ISO 17666:2016, ISO 11231:2019
Risk Tracking	AFI 63-101/20-101, AFPAM 63-128, and DoD RIO Guide, ISO 17666:2016, ISO 22311:2019

NOTE: During the risk identification process, if the threats and vulnerabilities analyses highlight any risks of accidental death, injury, or occupational illness, or a risk of destruction of defense and space systems, infrastructure, and property then hand off these risks to the safety community and continue to track these risks in regular monthly PM reviews to maintain traceability and accountability to the mitigation status. The safety community will then quantify and manage the risks via their MIL-STD-882 process. If appropriate, refer to AFPAM 63-128, Figure 12.3, *and Translation of MIL-STD-882 Risk Matrix to the OSD Risk Management Guide Matrix.*

- Cybersecurity and Cyber Resiliency process for risk management planning. Include a description of how system security risks will be managed in program risk management plans as per AFI 63-101/20-101 and AFPAM 63-128. SSE considerations to be included in the program's risk management plan include, but are not limited to:
  - Integration of adversary threats into the RM process.
  - Describe how SSE considerations are represented on the Risk Management Board (RMB) and Risk Working Group (RWG) or equivalent forum(s).

  - Include the SSE Technical Lead roles, responsibilities and authorities (e.g., Milestone Decision Authority (MDA), Authorizing Official (AO), SCA, USAF AT Lead, Anti-Tamper Evaluation Team (ATET), Trusted Systems and Networks (TSN) Focal Point, Defense Intelligence Agency (DIA) Threat Assessment Center (TAC), SSE Technical Lead, Cybersecurity Architect, Information Systems Security Manager (ISSM), Software Assurance Technical Lead, SCRM Technical Lead, etc.).

  - Show how SSE Workflow Processes and procedures integrate into overall programmatic Risk Management processes and procedures.

  - Ensure Critical Program Information (CPI) and Anti-Tamper risks are assessed in a forum appropriate for the classification of the information, as determined by the program's security classification guide.

  - Identify any SSE risk-related tools [e.g., Acquisition Security Database (ASDB), enterprise Mission Assurance Support Service (eMASS), DIA-TAC, list of Defense Microelectronics Activity (DMEA) accredited suppliers, Government-Industry Data Exchange Program (GIDEP)].

  - Describe any SSE risk evaluation and assessment methodologies that are different from programmatic risk assessment techniques (e.g., AO, SCA, USAF AT Lead, TSN Focal Point, DIA-TAC, etc.).

  - Include how SSE risks are going to be communicated and factored in to overall programmatic risk decisions.

- Considerations for identifying system security risks. A system security risk is developed when a potential threat could exploit a system vulnerability such that an adverse impact to mission accomplishment could occur. These are risks to the mission critical functions, safety critical functions, and functions associated with CPI as defined during the Functional Thread Analysis. For more details on identifying these critical functions, see Appendix C: Functional Thread Analysis. Possible potential sources of risk are provided by Table A-6.

Table A-5 Potential Sources of Risk

System Security Risk Area	Examples
Government organization	• Security practices • Untrained personnel • Malicious insiders • Insufficient or incorrect classification of information and dissemination handling control • Foreign Intel collection
Contractor organization and environment	• Facilities, including design, development, and production • Networks • Supply chains • Personnel • Protection of CPI/CC • Foreign Intel collection
Software and hardware	• Adversary attacking Logic-Bearing Components (LBC) at suppliers • Embedded malware • Malicious code pre-installed • Hiding backdoors and features for unauthorized remote access • Microelectronics used in the system or incorporated into spares • SW version from supplier different than tested/verified version • HW configuration from supplier different than tested/verified configuration • Exploitable Software Vulnerabilities
System interfaces	• All network and system interfaces • Adversary exploiting penetrations of the Platform Information Technology (PIT) boundary
Enabling and support equipment, systems, and facilities	• Test, certification, maintenance, design, development, manufacturing, or training systems, equipment, and facilities • External Mission Load Compromise • Malicious software update
Fielded systems	• Adversary or insider threat gaining physical access to system • Cyber-attack on the system and/or network • Adversary negatively impacting mission critical functions • Protection of CPI/CC • Exfiltration via removable media or external network • Reverse engineering of lost/stolen/captured components as well as exported systems • Capture or manipulation of life cycle sustainment/prognostics data
System Development	• Compromise design and/or fabrication of hardware components • Not utilizing recommended security controls • Issues with security controls highlighted during testing

The information below is required to be added to the RMP to ensure Cybersecurity and Cyber Resiliency are established and maintained. This Section does not include the Anti-Tamper consequence of compromise. Reference the Anti-Tamper Technical Implementation Guide (TIG) and the DoD CPI HPG separately for determining Anti-Tamper Consequence-of-Compromise (CofC).

The program will establish likelihood for system security risks. System Security risk likelihood will be determined by considering two factors:

1. Likelihood of Threat Occurrence – Threat Intent & Opportunity - an estimation of an adversary's likelihood to attack the system. Continuous input data from the Intel, threat reports, vulnerability assessments, and other risk factors provide more clarity as to what /how the adversary attacks your system. As you get a better understanding of how the attacker exploits your system weaknesses, and you assess your system resiliency, this provides the avenue to integrate more resilient solutions and if possible, an opportunity to redesign a more system survivable solution.

2. Likelihood of Threat Success – Threat Capability and Likelihood of Threat Event Success - an estimation of an adversary's capability in creating the conditions necessary for a risk occurrence, considering cost, time, and skill needed to execute a successful attack. Once the threat vector is understood and proper mitigations applied, this increases your system resiliency and in turn, system survivability and then reduces the chances of a particular threat event succeeding.

Table A-6 Likelihood of Threat Occurrence

Likelihood of Threat Occurrence	
AFPAM 63-128	**Likelihood of Threat Event Initiation (Adversarial) or Occurrence (Non-Adversarial)**[12]
Near Certainty	Adversary is almost certain to initiate the threat event. The threat event/actor or Tactic, Technique, or Procedure (TTP) has been seen by the system or mission area.
Highly Likely	Adversary is highly likely to initiate the threat event. The threat event/actor or TTP has been seen by the organization's peers.
Likely	Adversary is somewhat likely to initiate the threat event. The threat event/actor or TTP has been reported by a trusted source.
Low Likelihood	Adversary is unlikely to initiate the threat event. The threat event/actor or TTP has been predicted by a trusted source.
Not Likely	Adversary is highly unlikely to initiate the threat event. The threat event/actor or TTP has been described by a somewhat credible source.

Table A-7 Likelihood of Threat Success

[12] Tailored version of NIST SP800-30 Table E-4, Relevance of Threat Events and DoD Risk Assessment Guide, Table 2-10

Likelihood of Threat Success	
AFPAM 63-128	**Likelihood of Threat Events Resulting in Adverse Impacts[13]**
Near Certainty	Threat has a very high capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is almost certain to succeed.
Highly Likely	Threat has a high capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is highly likely to succeed.
Likely	Threat has a moderate capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is likely to succeed.
Low Likelihood	Threat has a low capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it is has a low likelihood to succeed.
Not Likely	Threat has a very low capability of success to exploit the vulnerability. If the threat event is initiated or occurs, it has a very low likelihood to succeed.

NOTE: Likelihood values can be also represented by semi-quantitative values if desired: Not Likely = 1-4%, Low Likelihood = 5-20%, Likely = 21-79%, Highly Likely = 80-95%, Near Certainty = 96-100%.

[13] Tailored combination of NIST SP800-30, Table D-3, Characteristics of Adversary Capability and NIST SP800-30, Table G-4

Combining the two factors of Likelihood of Threat Occurrence from Table A-7 and Likelihood of Threat Success from Table A-8 (NIST SP800-30 r1.0, Table G-5) results in the system security risk likelihood factor for Life Cycle Risk Management (LCRM) analysis, i.e., the "likelihood" as shown in Table A-9.

Table A-8 Risk Likelihood

Likelihood						
Likelihood of Threat Occurrence (Table 1.10-4)	Near Certainty	2	3	4	5	5
	Highly Likely	2	3	4	5	5
	Likely	1	2	3	4	5
	Low Likelihood	1	2	3	4	4
	Not Likely	1	1	2	3	3
		Not Likely	Low Likelihood	Likely	Highly Likely	Near Certainty
		Likelihood of Threat Success (Table 1.10-5)				

The program will establish consequence for system security risks. System Security risk consequence will be determined by considering two factors. This risk will be assessed for the system before mitigations are applied, and reassessed after mitigations are applied.

1. Vulnerability Severity - an estimation of the damage to the system resulting from exploitation of a vulnerability by an adversary, stated in terms of loss of capability, disruptive system change or loss of information. This data comes from vulnerability assessments.
2. Mission Criticality - an estimation of adverse effects to the mission, organization, assets, individuals, or nation due to system/capability/information loss or compromise. This data comes from mission thread and system criticality analyses.

Table A-9   Vulnerability Severity

Vulnerability Severity	
AFPAM 63-128 (Tailored)	**AFLCMC Standard Process for Cybersecurity A&A**
Severe/ Catastrophic	The vulnerability is of severe/catastrophic concern. Vulnerability exploitation results in severe/catastrophic system performance impact, and/or severe compromise or modification of the system information.
Significant	The vulnerability is of significant concern. Vulnerability exploitation causes significant unacceptable system capability impact and/or significant compromise or modification of the system/system information.
Moderate	The vulnerability is of moderate concern. Vulnerability exploitation causes partial system performance impact and/or partial compromise or modification of the system/system information.
Minor	The vulnerability is of minor concern. Vulnerability exploitation causes minor system capability impact and/or minor compromise or modification of the system/system information.
Minimal	The vulnerability is of minimal concern. Vulnerability exploitation causes minimal system performance impact and/or no compromise or modification of the system/system information.

Table A-10 Mission Criticality

Mission Criticality	
AFPAM 63-128 Tailored	**Combining Protection Failure Criticality Levels for DAG with information classification level verbiage.**[14]
Severe/ Catastrophic	Loss of the system/subsystem/function/capability results in Severe or Total Mission Failure and/or compromise or loss of information results in exceptionally grave damage to national security.
Significant	Loss of the system/subsystem/function/capability results in Significant/Unacceptable Mission Degradation and/or compromise or loss of information results in grave damage to national security.
Moderate	Loss of the system/subsystem/function/capability results in Moderate or Partial Mission Degradation and/or compromise or loss of information results in damage to national security.
Minor	Loss of the system/subsystem/function/capability results in Minor Mission Degradation and/or compromise or loss of information results in limited damage to national security.
Minimal	Loss of the system/subsystem/function/capability results in Minimal Mission Degradation and/or compromise or loss of information results in negligible damage to national security.

[14] Protection Failure Criticality Levels for DAG, Chapter 9, Table 3, and TSN Analysis (June 2014), Table 2-1

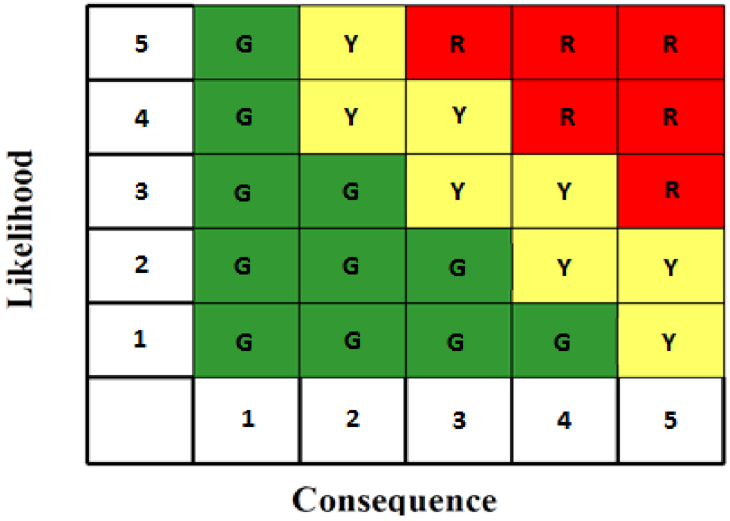
Combining the two factors of Vulnerability Severity and Mission Criticality using NIST SP800-30 r1.0, Table G-5 results in the system security risk consequence factor for LCRM analysis as shown in Table A-12.

Table A-11 Risk Consequence

Consequence						
Vulnerability Severity (Table 1.10-7)	Severe/ Catastrophic	2	3	4	5	5
	Significant	2	3	3	4	5
	Moderate	1	2	3	4	5
	Minor	1	1	2	3	4
	Minimal	1	1	1	2	3
		Minimal	Minor	Moderate	Significant	Severe/ Catastrophic
		Mission Criticality (Table 1.10-8)				

The program will determine risk level for system security risks. Once the system security risk likelihood and system security risk consequence factors are determined using the procedures above, the risk level will be determined using the life cycle risk management 5X5 risk matrix process described in AFPAM 63-128, para 12.2.4.6 and Figure 12.2, and AFI 63-101/20-101, para 4.6.1.1 and Figure A3.2.

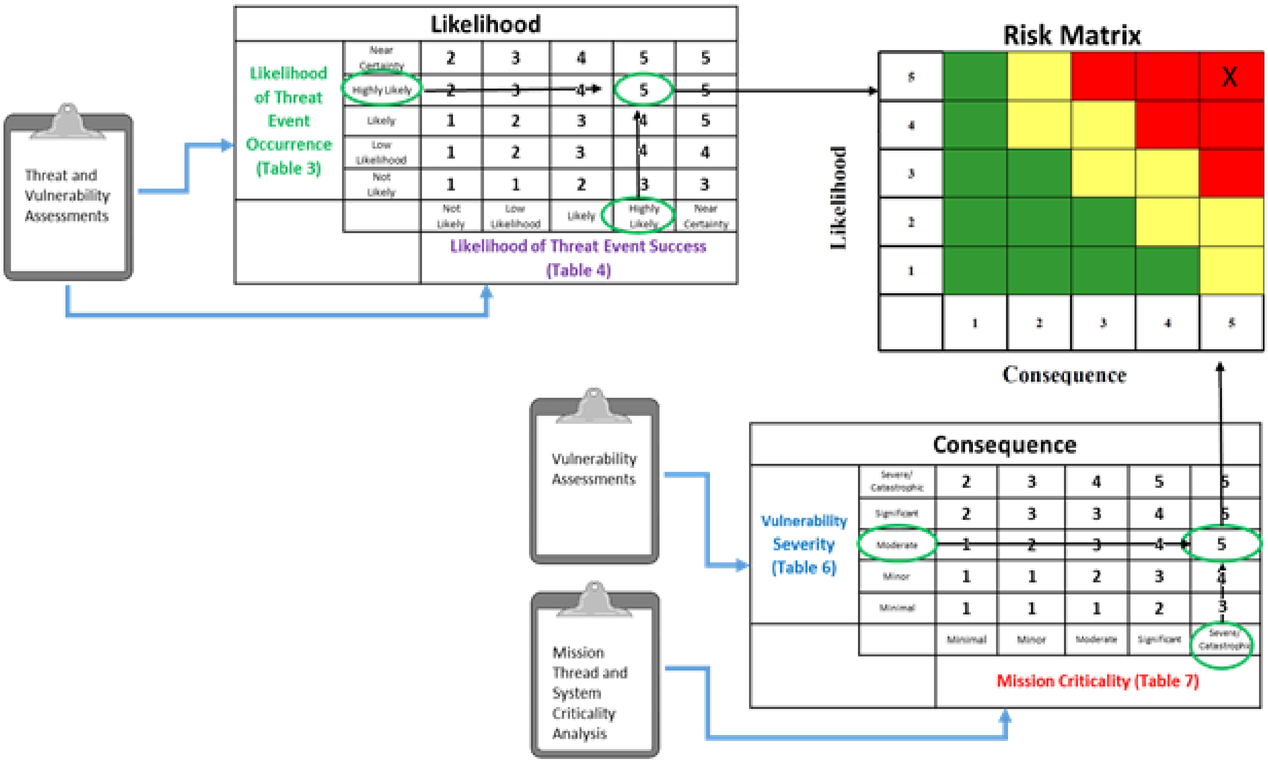
Table A-12 Risk Matrix



Likelihood	5	G	Y	R	R	R
	4	G	Y	Y	R	R
	3	G	G	Y	Y	R
	2	G	G	G	Y	Y
	1	G	G	G	G	Y
		1	2	3	4	5
		Consequence				

NOTE: Security risk must be marked, stored and handled as per the Security Classification Guide (SCG) of the program.

Worked Example: Figure A-3 graphically shows how to flow through the system security risk assessment step of the risk management process.


Threat and Vulnerability Assessments
Vulnerability Assessments
Mission Thread and System Criticality Analysis
Risk Matrix
Likelihood
Consequence

Likelihood

Likelihood of Threat Event Occurrence (Table 3)						
	Near Certainty	2	3	4	5	5
	Highly Likely	2	3	4	5	5
	Likely	1	2	3	4	5
	Low Likelihood	1	2	3	4	4
	Not Likely	1	1	2	3	3
		Not Likely	Low Likelihood	Likely	Highly Likely	Near Certainty
		Likelihood of Threat Event Success (Table 4)				

Risk Matrix

5	🟩	🟨	🟥	🟥	X
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

Consequence

Vulnerability Severity (Table 6)						
	Severe/ Catastrophic	2	3	4	5	5
	Significant	2	3	3	4	5
	Moderate	1	2	3	4	5
	Minor	1	1	2	3	4
	Minimal	1	1	1	2	3
		Minimal	Minor	Moderate	Significant	Severe/ Catastrophic
		Mission Criticality (Table 7)				

Figure A-3 Risk Assessment Example

1.11. Systems Engineering Plan (SEP)

The SEP is prepared by the PO and is a living document that details the execution, management, and control of the technical aspects of an acquisition program from conception to disposal. The details of SSE planning, including the Cybersecurity Strategy, can be found in the PPP. The Cybersecurity requirements are derived from the operational mission of the system, classification and criticality of individual system components, as well as, the CSAs, and the applicable security controls. The Cybersecurity requirements, derived from the CSAs, can be found in the SRD or system specification. Consider all the factors listed in Table A-14 when planning SSE activities for the program.

Table A-13 Factors to Consider When Planning SSE Activities

SSE Activity Planning Factors	
• Critical Program Information (CPI)	• Anti-Tamper (AT)
• Cybersecurity	• Cyber Resiliency
• Exportability features	• Operations security (OPSEC)
• Information security (INFOSEC)	• Personnel security (PERSEC)
• Physical security	• Secure system design
• HwA	• SwA
• Anti-counterfeit practices	• SCRM
• Cyber Survivability	• DoD Mission Engineering Guidebook

Include SSE considerations in the following SEP Section(s):

- Section 1, “Introduction.” – Describe the approach to align Government SSE activities with the contractor’s Program Protection Implementation Plan (PPIP) and/or Systems Engineering Management Plan (SEMP). List relevant supporting programmatic documentation (PPP and Cybersecurity Strategy, TEMP, RMP, System Spec, LCSP, etc.) and describe the aspects of SSE captured in each of them.

- Section 2.1, “Architectures and Interface Control.” – List the products that will be developed, to include system level system security, physical, software, and DODAF architectures. Include Cybersecurity and Cyber Resiliency (Cybersecurity, Cyber Resiliency, Anti-Tamper/Critical Program Information, and Trusted Systems and Networks), as described in the SRD/Specification Section for thread analysis or criticality analysis, in the architectures and IS-ICDs that meet the program requirements. Identify any Cybersecurity and Cyber Resiliency dependencies with other weapons, space, and/or ground systems, and/or systems security enterprise services.

- Section 2.2, “Technical Certifications, Table 2.2-1.” – Summarize any SSE-related certifications which must be obtained during program's life cycle (e.g., CCA Compliance Report, CS KPP, Cybersecurity, AT, NSA Type-1 CRYPTO, Cross Domain Solution (CDS), etc. certifications).

- Section 3.1, “Technical Schedule and Schedule Risk Assessment.” – Include any SSE-related schedule impacts and/or interdependencies (e.g., AT verification, use of trusted suppliers, counterfeit parts testing, third-party HwA and/or SwA, etc.). Ensure SSE events are captured on Figure 3.1-1 System Technical Schedule.

- Section 3.2, “Engineering Resources and Cost/Schedule Reporting.” – Ensure both Government and contractor schedules and WBSs reflect SSE-related activities and interdependencies. Ensure SSE events are traceable to the Statement of Work (SOW), WBS, Integrated Program Management Report (IPMR), and Contractor Work Breakdown Structure (CWBS).

- Section 3.3, “Technical Risk and Opportunity Management.” – Ensure SSE risks are captured as part of the Government and contractor risk management processes. This should include how the PO will identify and analyze key SSE risks; and plan for, implement (including funding), and track risk mitigation. Include any SSE-related opportunities that can yield improvements in the program’s cost, schedule, and/or performance baseline through reallocation of resources. Software unique risks to include software obsolescence (DMs) should be addressed. Often ignored are the risks associated with manufacturing data and drawing changes to the design data and drawings. The Manufacturing BOM, sparing and warranties, licensing, and the retirement of space and weapon systems component and eventually, the space and weapon systems themselves. Also, include consideration of the SSE-related threats in an operational environment throughout all phases of the program.

- Section 3.4, “Technical Organization.” – Ensure Government and contractor organizations have identified and funded SSE staffing levels. Include the SSE Technical Lead in the program’s technical staffing plan and organizational charts. Describe impacts from any SSE-related staffing shortfalls and what the PO is doing to address the shortfall. Ensure inclusion of SSE across the IPT organization listed in Table 3.4.4-2 IPT Team Details (e.g., risk management, T&E, V&V, SE, logistics, sustainment, etc.).

- Section 3.5, “Relationships with External Technical Organizations.” – Include SSE considerations in the processes or methods used to document, facilitate, and manage interaction among SE team(s), external-to-program Government organizations (e.g., AO, USAF AT Lead, ATET, NSA, DIA, Air Force Office of Special Investigations (AFOSI), etc.). Also, include any SSE-required GFE/GFP/Government Furnished Information (GFI) (e.g., Cybersecurity test ranges, AT integration laboratories, cryptography, Trusted Foundry, and SSE special equipment). Strong consideration should be given to including a ‘strategy-to-task’ decomposition of SSE-related adversary threats, derived from validated threat, as GFI.

- Section 3.6, “Technical Performance Measures (TPM) and Metrics.” – Include set of SSE-related TPMs and intermediate goals, and the plan to achieve them with as-of dates (to provide quantitative insight into requirements stability and specification compliance). Examples include SSE-related TPMs in the areas of software, reliability, manufacturing, and integration to assess "performance to plan." Describe the traceability between SSE-related KPPs, KSAs, key technical risks and identified TPMs, or other measures.

- Section 4, "Technical Activities and Products." – Include any SSE-related activities, design reviews, entry/exit criteria, and design considerations. Include a description of the process for the identification of CPI/CC and identification of critical components required to implement SCRM countermeasures. Include a plan for collecting software assurance evidence.
- Section 4.3, "Requirements Development and Change Process." – Describe how SSE requirements derived from system survivability KPP, Cyber Survivability Attributes (CSAs), and security controls will be included in the SRD/System Specification and managed the same as all other program requirements.
- Section 4.4, "Technical Reviews." – Identify SSE related Entry and Exit criteria for all technical reviews; ensure these criteria are appropriate to the expected maturity level of the program for when the review is scheduled to be conducted.
- Section 4.6, "Design Considerations." – Ensure the SEP includes SSE-related design considerations, including trade study criteria (e.g., how design will address safeguarding CPI/CC, how the architecture and specification requirements are derived, traced, and support the Cybersecurity and Cyber Resiliency requirements, provide HwA, SwA, countermeasures against threats, integrate SCRM into life cycle sustainment processes, which open standards are being considered, etc.). Describe how the design addresses protection of DoD warfighting capability from foreign intelligence collection; from hardware and software vulnerabilities, and supply chain exploitation; and from battlefield loss throughout the system life cycle, balancing security requirements, designs, testing, and risk management in the respective trade spaces. Include in Table 4.6-1, Design Considerations.
- Section 4.7, "Engineering Tools." – Identify any SSE-related tools the program plans to use (e.g., CWE™, CVE®, and CAPEC™, etc.). Also, ensure SSE considerations are included in the use of SE tools (e.g., Dynamic Object-Oriented Requirements System (DOORS), Requirements Traceability Verification Matrix (RTVM), Risk Management Information System (RMIS), etc.) is included in Table 4.7-1, Engineering Tools.
- Annex A "Acronyms." – Include any SSE-related acronyms.

1.12. Test and Evaluation Master Plan

The Test and Evaluation Master Plan (TEMP) describes the program's T&E strategy throughout the acquisition life cycle. Its development is led by the Chief Developmental Tester (CDT) with significant inputs from the Integrated Test Team (ITT) and SSE team. These personnel provide the necessary test and SSE-related technical, operational, and programmatic expertise to ensure functional and security requirements are verified through the appropriate means – demonstration, inspection, analysis, and test. It starts with Technology Development (TD) and continues through Engineering, Manufacturing and Development (EMD) into the Production and Deployment (PD) Phase. The TEMP is submitted for approval prior to Milestone A and is updated at the Development RFP Release decision, Milestone B, Milestone C, and Full-Rate Production (FRP)/Fielding Decision (FD), as well as, for BCAC Authorization to Proceed (ATP) decisions.

Include SSE considerations in the following TEMP Section(s) (additional TEMP development guidance is available in the Director, Operational Test and Evaluation [DOT&E], Test and Evaluation Master Plan Guidebook and the Air Force Cyber Test and Evaluation Strategy Template):

- **Section 1.2**, "Mission Description." – Include significant SSE-related points from the Life Cycle Sustainment Plan, the ISP, and the PPP. Describe the operational environment from an SSE-perspective, to include other systems that exchange information with the system under test; includes the network environment, end-Users, administrators, cyber defenders, and cyber threats.

- **Section 1.3**, "System Description." – Include key SSE-related features and subsystems, both hardware and software (e.g., the security architecture, security classification levels, CSSPs, open standards, etc.). Include the system's security categorization [IAW DoDI 8510.01 and by reference, Committee on National Security Systems Instruction (CNSSI) No. 1253] in terms of the impact values for confidentiality, integrity, and availability. Describe any previous SSE certifications/assessments (e.g., Cybersecurity, AT, HwA, SwA, cryptography, etc.) and prior system authorizations. Include any interconnections between major subsystems (e.g., Ethernet links, etc.), external connections (e.g., NIPRNET, SIPRNET, etc.), and any physical access points (e.g., USB ports, etc.).

- **Section 1.3.4**, "System Threat Assessment." – Summarize the threat environment in which the system must operate. Examine system architecture products (e.g., SV-1 Systems Interface Description, SV-6 Systems Resource Flow Matrix, etc.) to identify interfacing systems, services, and data exchanges that may expose the system to potential threat exploits. Emphasis should be placed on adequate representation of threats, threat attributes, and threat environments that are most relevant to the evaluation of the system under test, including evaluation of system lethality and survivability. Perform a preliminary appraisal of threats and threat attributes that are likely to have the greatest impacts on operational effectiveness. Reference the appropriate STAR and/or VOLT, DIA, AFOSI, or component-validated threat documents for the system. If validated threat documents are lacking sufficient detail to characterize SSE-related adversary threats to system attack surfaces, consult with the supporting acquisition intelligence organization (SMC/IN, AFNWC/NT2, AFLCMC/IN, NASIC, or other acquisition intelligence unit) for additional support.

- **Section 1.3.5**, "Systems Engineering (SE) Requirements." – Include any SSE-related information and activities that will be used to develop the TEMP.

- **Section 1.3.6**, "Special Test or Certification Requirements." – Identify unique system characteristics or support concepts that will generate special test, analysis, and evaluation requirements (e.g., system security assessments, Cybersecurity authorizations, HwA & SwA assessments, penetration testing, post deployment software support, AT resistance to Reverse Engineering (RE)/exploitation efforts, counterfeit parts testing, etc.). Indicate if the threat assessment reveals that critical threats, targets, or threat attributes are not available to support operational or live-fire testing. Describe the need for development of special threat or target systems and any activities necessary to validate these systems for use in testing.

- **Section 2.1**, "T&E Management." – Include any SSE-related key roles and their responsibilities. Ensure SSE-related personnel are included in the T&E management structure, to include the sub-workgroups.

- **Section 2.2**, "Common T&E Database Requirements." – Describe the requirements for and methods of collecting, validating, and sharing data as it becomes available from the contractor, Developmental Test (DT), Operational Test (OT), and oversight organizations, as well as, supporting related activities that contribute or use test data (e.g., SSE countermeasures - AT, Cybersecurity, HwA, SwA, etc.). Describe how the pedigree of the data will be established and maintained. The pedigree of the data refers to understanding the configuration of the test asset, and the actual test conditions under which the data were obtained for each piece of data. Identify who will be responsible for maintaining this data.

- **Section 2.3**, "Deficiency Reporting." – Include the processes for documenting and tracking SSE-related deficiencies (e.g., malicious code, counterfeit parts, etc.) identified during system development and testing into Joint Deficiency Reporting System (JDRS). Describe how the information is accessed and shared across the program. The processes must address SSE-related problems or deficiencies identified during both contractor and Government test or verification activities. The processes must also include issues that have not been formally documented as a deficiency (e.g., watch items). If needed, the PO should develop a response plan for reporting classified deficiencies.

- **Section 2.5**, "Integrated Test Program Schedule." – Include any SSE-related (e.g., AT, cryptography, Cybersecurity, HwA, SwA, SCRM, etc.) T&E (and AT verification) major decision points, related activities, and planned cumulative funding expenditures by year. Also, include significant Cybersecurity event sequencing, such as Interim Authorizations to Test (IATTs) and ATOs. Include on Figure 2.1.

- Section 3.1, "T&E Strategy." – Include SSE considerations in the summary of an effective and efficient approach to the test program (e.g., use of Cybersecurity BLUE and RED Teams, use of independent third-party HwA, SwA, SCRM, or AT audits/analyses/assessments, etc.). Focus on the testing for SSE capabilities, and address testing of subsystems or components where they represent a significant risk to achieving a necessary secure capability. Identify test opportunities in which representative systems and services will be available to conduct protection-related testing in a system-of-systems context, such as Joint Interoperability and Test Command (JITC) interoperability testing.

- **Section 3.2**, “Evaluation Framework.” – Ensure SSE-related verification considerations are included in the overall evaluation approach focusing on key SCRM decisions and addressing key SSE-related system risks and issues. The evaluation should encompass prevent, mitigate and recover cyber defense functions.

- **Section 3.2.1**, “Developmental Evaluation Approach.” – Ensure the Developmental Evaluation Framework includes which test activities (i.e., Cyber T&E Phase 2, 3, and 4 activities) will be used to inform the Decision Support Questions (DSQs). The selected test activities should be appropriate to the anticipated level of system maturity and generate the desired test data to inform the respective DSQs (refer to Table 6-2 in the DoD Cybersecurity Test and Evaluation Guidebook for a list of CVI activities).

- **Section 3.2.2**, “Developmental Test Events.” – Ensure the anticipated CVI and ACD schedule is outlined and aligns with the system development strategy/timeline (the Phase 3 CVI typically includes several events executed at various points in system’s development process whereas the Phase 4 ACD typically consists of one or two events late in the DT phase). If the CVI event timing is not program schedule driven, identify the events that will drive the CVI schedule. Describe any planned contractor cyber testing, integrated contractor-Government cyber testing, and integrated cyber DT-OT and how it will align with SSE activities. Identify which events will generate cyber test data to support the follow-on Adversarial Cyber Developmental Test and Evaluation (ACD), Cooperative Vulnerability and Penetration Assessment (CVPA), and Adversarial Assessment (AA) test objectives. For the ACD, identify how the ACD test scope will be determined (e.g., high priority Attack Path Vignettes generated during the United States Air Force, MBCRA iteration), the scope of cyber test, cyber test resources required/anticipated to execute the planned ACD events, and when the ACD will occur. If the ACD event timing is event driven, describe the event(s) that will drive the ACD timing. Identify any integrated and/or combined cyber test events that will provide data to support the ACD test objectives. Finally, identify which cyber test agency(s) will conduct the CVI and ACD activities, and the environment(s) the CVI and ACD test events will be conducted.

- **Section 3.2.3**, “Test Limitations.” – Include any SSE-related test limitations that will impact DT, to include functional and cyber testing (e.g., test scope limitations/restrictions, classification issues, threat realism, resource availability, limited operational environments, limited support environment, maturity of tested systems or subsystems, etc.) , as well as, the planned limitation mitigations and the resultant impacts upon test. Describe any critical threats, targets, or threat attributes identified during the threat assessment that are not expected to be available to support developmental testing.

- **Section 3.3**, “Integrated Test Approach.” – Ensure the SSE-related approach to testing the system performance in a mission context is incorporated into the DT strategy. Include any SSE-related certifications or approvals required (e.g., Cybersecurity, AT, COMSEC, cryptography, trusted suppliers, third-party HwA or SwA assessments, etc.). Quantify the SSE-related testing sufficiently (e.g., number of test hours, test articles, test events, test firings, etc.) to allow a valid cost estimate to be created. Discuss plans for interoperability and Cybersecurity testing, including the use of cyber ranges for vulnerability and adversarial testing. Explain how SSE activities will impact T&E (e.g., rapid incorporation of system adjustments to remediate/mitigate cyber vulnerabilities/functional deficiencies and plan to adjust test execution to validate effectiveness of system changes.)

- **Section 3.3.2**, "Developmental Test Events." – For systems that are mature enough to participate in a realistic network environment in an operationally representative configuration, describe how the program will integrate Cooperative Vulnerability and Penetration Assessments (CVPAs) into the developmental phase of testing. If so planned, identify when and where the CVPAs will be conducted, which Operational Test Agency (OTA) will conduct the CVPA, and ensure DOT&E approval of the CVPA plan.

- **Section 3.4**, "Certification for Initial Operational Test & Evaluation (IOT&E)." – Identify any SSE-related considerations necessary to ensure the system will be certified safe and ready for IOT&E, such as completion of any SSE-related assessments (e.g., Cybersecurity, Cyber Resiliency, AT, COMSEC, cryptography, use of independent third-party HwA, SwA or SCRM audits/ analyses/assessments), prior system authorizations, and completion of any SSE security-related assessments.

- **Section 3.5**, "Operational Evaluation Approach." – Ensure the OT strategy will adequately assess SSE focus areas in support of mission effectiveness, suitability, and survivability. Define Cybersecurity measures and criteria for prevent, mitigate, and recover in this Section or in the Cyber Appendix (typically Appendix E). This should include all cyber OT measures, as well as, any programmatic measures that should be assessed during OT. Include any SSE-related considerations in the approach to conducting the independent evaluation of the system.

- **Section 3.5.1**, "Operational Test Events and Objectives." – Ensure the key SSE-related operational test objectives are included in the appropriate test event(s) and test phases. Include a detailed, SSE-relevant diagram indicating which elements are included (inside the test boundary) or excluded from test (e.g., major subsystems, all connections including their protocols, all physical access points, etc.). Identify when the CVPA(s) and AA(s) will be conducted. Highlight any anticipated integrated test data that will be used to fulfill OT requirements. Ensure the SSE-related data collection methods are articulated (i.e., automated scanning/exploitation tools, physical inspection, document reviews, and personnel interviews). Identify all SSE-related data and metrics to be collected. Identify which agencies will conduct the CVPA(s) and any items that will be tested that were not tested during DT (e.g., operational interfaces not available in the DT environment). For the AA, ensure the cyber test agencies that will conduct the AA are identified, as well as, when the AA is expected to occur. NSA-certified and United States Cyber Command (USCYBERCOM)-accredited teams are required to evaluate systems connected to the DoDIN. Identify the team responsible for collecting prevent, mitigate, and recover data from both local and non-local (e.g., Tier 2) cyber defenders. Specify the duration of the assessment(s). Document the Intelligence Community recognized cyber threat and specify whether the mission effects of the adversarial attack will be assessed by direct measurement of the effect on system performance parameters or an assessment by independent Subject Matter Experts (SMEs). Specify who will act as the local and higher-tier cyber defenders to provide detect and react data. If SMEs will assess the mission effects, briefly describe their proposed methodology.

- **Section 3.5.2**, "Operational Evaluation Framework." – Ensure the SSE-related goals of the operational test are identified and expressed in a mission context. Identify planned sources of SSE-related information (e.g., developmental testing, testing of related systems, modeling, simulation, etc.). Identify the SSE-related critical issues and describe the evaluation criteria for each test.

- **Section 3.5.4**, "Test Limitations." – Include any SSE-related test limitations that will impact OT (e.g., test scope limitations/restrictions, classification issues, threat realism, resource availability, limited operational environments, limited support environment, maturity of tested systems or subsystems, etc.) , as well as, the planned limitation mitigations and the resultant impacts upon test. Describe any critical threats, targets, or threat attributes identified during the threat assessment that are not expected to be available to support operational or live-fire testing.

- **Section 3.7**, "Other Certifications." – Identify SSE-related key testing prerequisites and entrance criteria, such as required SSE-related approvals (e.g., Cybersecurity, AT, COMSEC, cryptography, use of trusted foundry, use of third-party hardware, firmware, and software assessments, etc.).

- **Section 4.2**, "Test Resource Summary." – Include any SSE-related resources necessary to accomplish the T&E program and SSE-related test resources (e.g., instrumentation, support equipment, test ranges/facilities, threats, special requirements, use of third party audits/analyses/assessments, etc.), any shortfalls, impacts to planned testing, and approach to resolving shortfalls.

- **Section 4.2.5**, "Threat Representation." – Identify the SSE-related type, number, availability, requirements, and schedule for all SSE-related threat representations to be used in testing.

- **Section 4.2.10**, "Special Requirements." – Include any SSE-related special requirements, items impacting the T&E strategy or Government test plans that must be put on contract or which are required by statute or regulation, top-level SSE-related activities the contractor is responsible for, and the kinds of support that must be provided to Government testers (e.g., Cybersecurity, AT, COMSEC, cryptography, use of trusted foundry, use of third-party hardware, firmware and software assessments, etc.).

- **Section 4.3**, "Manpower/Personnel and Training." – Include any SSE-related manpower/personnel, travel, and training requirements (e.g., use of SCAs, ATET, use of third-party HwA, SwA or SCRM audits/analyses/assessments, trusted foundry, trusted suppliers, etc.), as well as, limitations that may affect T&E execution.

- **Section 4.4**, "Test Funding Summary." – Include SSE-related test resources/costs (e.g., trusted foundry, temporary duty (TDY)/travel, Cybersecurity test ranges/facilities, specialized test facilities, use of third-party HwA, SwA or SCRM audits/analyses/assessments, ATET, etc.), and sources of funding.

- **Appendix A**, “Bibliography.” – Include any SSE-related references.

- **Appendix B**, “Acronyms.” – Include any SSE-related acronyms.

- **Appendix C**, “Points of Contact.” – Include the Lead SSE and any other SSE-related points of contact (POCs).

- **Appendix E**, “Cybersecurity.” – This Appendix is not required if SSE-related considerations are already stated in the body of the TEMP.

- **Appendix G**, “Requirements Rationale.” – If SSE-related requirements are not adequately documented in the IS-CDD or other requirement documents, add rationale to this Appendix. In these cases, the SSE requirements may be derived or transformed for testability, or the operational rationale is unclear. This Appendix should explain the operational rationale and/or the derivation of the metric, as well as, the chosen numerical thresholds.

1.13. Work Breakdown Structure

A 1.13. Work Breakdown Structure (WBS)[15] is a tool to represent the entire “break down” of a program and is used for planning, cost estimating, execution, and control. Separate WBSs are prepared by both the PO and by the contractor. SSE tasks and deliverables are included in both WBSs. The Contractor Work Breakdown Structure (CWBS) aligns with the SOW. See the **Statement of Objectives (SOO) and Statement of Work (SOW)** section of this document.

2.0. Requirements Documents

The Government, as part of the acquisition process, develops the following documents.

2.1. Performance Work Statement

A Performance Work Statement (PWS) is written by the PO for performance-based acquisitions (i.e. services contract). A PWS is usually a part of an Advisory and Assistance Services (A&AS), Systems Engineering and Technical Assistance (SETA), and Federally Funded Research and Development Centers (FFRDCs) contract. These are service contracts, which directly engages the time and effort of a contractor whose primary purpose is to perform an identifiable task rather than to furnish an end item of supply. It clearly describes the performance objectives and standards that are expected of the contractor. When a contract is awarded, the PWS is legally binding upon the contractor and the Government. A PWS should state requirements in general terms of what (result) is to be done, rather than how (method) it is done. It is written in “active” versus “passive” voice. A PWS gives the contractor maximum flexibility to devise the best method to accomplish the required result. It must be written to ensure that all Offerors compete equally. A PWS must also be descriptive and specific enough to protect the interests of the Government and to promote competition. A definitive PWS is likely to

[15] MIL-STD-881

produce definitive proposals, thus reducing the time needed for proposal evaluation. If applicable, include SSE considerations in the following PWS Section(s):

- **Section 1**, “Introduction.” – Describe the overall acquisition vision and desired mission results. Set expectations for contractor performance in terms of teamwork and improving mission results thru efficiencies and process improvements.
- **Section 2**, “Background Information.” – Briefly describe the scope of the performance requirement and the desired outcome. Provide a brief historical description of the program/requirement that provides the context for the effort (include who is being supported and where). Describe the general desired SSE outcomes. As an example, if the task involves SSE assessments, provide a high-level overview of the number and characteristics (e.g., size and complexity) of the systems involved.
- Section 3, “Performance Objectives and Standards.” – Describe general SSE performance objectives that have an impact on the success of the mission (e.g., place of performance, period of performance, security clearance requirements, etc.). Use the High-Level Objectives (HLOs), tasks, and standards from the roadmap and transfer into the PWS. Include SSE standards to which the task must be completed.
- **Section 4**, “Applicable Documents.” – Include a listing of all applicable SSE-related documents and/or directives.
- **Section 5**, “Special Requirements/Constraints.” – Include information on any SSE-related GFP or GFE. Also, include any special SSE-related information, requirements, special work hours, and contingency requirements. If necessary, include a transition plan.
- **Section 6**, “Deliverables.” – Describe SSE-related deliverables, such as data requirements, reports or any other items contained within a Contract Data Requirements List (CDRL).

EXAMPLE - Information to Consider When Developing a PWS:

- *What SSE-related tasks must be performed to accomplish the desired outcomes?*
- *How are SSE-related tasks accomplished now? (e.g., essential inputs, processes, and outputs for each task.)*
- *For each SSE-related requirement, what measures of quality, quantity, and/or timeliness are appropriate and reasonable? What tolerance or deviation (if any) from the performance standards should be permitted?*
- *What method of surveillance or measurement will be used to determine whether identified performance standards and acceptable quality levels have been met?*

2.2. System Requirements Document, and System and Lower Level Specifications

The System Requirements Document (SRD) consists of system-level requirements that have been derived from User capability requirements documented in the IS-ICD, IS-CDD, or the Air Force Form 1067 for System Modifications. The SRD is the top-level acquisition requirements documentation from which detailed design specifications are derived. During system acquisition, the SRD is used to communicate the required functional, performance and behavioral aspects of a system to potential developers from industry. Once a contract to develop the system is awarded, the SRD becomes a contractually binding agreement between the Government and contractor that defines all data, and functional and behavioral requirements of the system under development. SRD requirements are stated in performance or functional terms, and do not specify design solutions. The SRD's purpose is to communicate the Government's requirements to industry in the RFP. A contractor providing a proposal in response to the RFP should respond to each requirement of the SRD with a system specification requirement that is verifiable and suitable for incorporation in the resulting contract. In some instances, the Government may provide a System Specification directly to the contractor. All requirements need to be approved by the Chief Engineer.

Per the **SSE Workflow Process in the SOO/SOW**, Section 2.3 of this document, all programs are required to document how Cybersecurity and Cyber Resiliency requirements are derived and traced between the SRD, and system and lower level specifications from the following documents:

- Cybersecurity through NIST SP800-53 controls per DoDI 8500.01 and DoDI 8510.01 as agreed by the Authorizing Official (AO).
- Trusted Systems and Networks (TSN) per DoDI 5200.44.
- Anti-Tamper (AT) Plan per ATEA responsibilities in DoDD 5200.47E and agreed by the USAF AT Lead.
- Cyber Resiliency per the User documentation (Information Security Initial Capability Document (IS-ICD), Information Security Capability Development Document (IS-CDD), and/or Air Force Form 1067 – see JCIDs Section for more details).

The **Cybersecurity and Resiliency SRD / System Specification requirements** should be derived from the User requirements document, see the JCIDs requirements to meet the System Survivability KPP and CSAs**. Section 1.1.6** provides the process the User and HPT should take to get to the appropriate protection requirements for each of the Mission Critical Functions (MCF), Safety Critical Functions (SCF) and the functions associated with CPI. The SE and SSE will be able to derive the appropriate requirements to put in the SRD and/or System Specification utilizing the Functional Thread Analysis, Top Level Architecture, the System Survivability KPP - CSAs, and the “System Reqs” worksheet in the Excel file found in **Attachment 1** of this document.

The MCF, SCF, and functions associated with CPI should be evaluated based on risk per Section 1.10 of this guidebook. The higher the risk indicates the need for mitigation through the application and implementation of the requirements in **Attachment 1** (i.e., the potential for more “lower-level” requirements).

In addition, the SEs and SSEs will flow down the requirements appropriately through the SSE Workflow Processes. Refer to Section 17.1. System Engineering Technical Reviews (SETRs) / Integrated Master Plan (IMP) for more information.

Finally, SEs and SSEs will update the Functional Thread Analysis (FTA) and the architecture to the lowest level through the SSE Workflow Processes. Lower-level requirements are located in Attachment 1 of this document, under the CSA 01-10 worksheets in the excel file. Refer to **Appendix B: USAF Combined Process Guide for CPI/CC Identification** for additional information to finalize the Functional Thread Analysis.

System requirements will be utilized when producing a new space and weapon system, but may also apply to modifications of an existing system. Lower-level requirements will be utilized during requirements derivation for subsystems and Line Replaceable Units (LRUs) as depicted in Figure A-4.

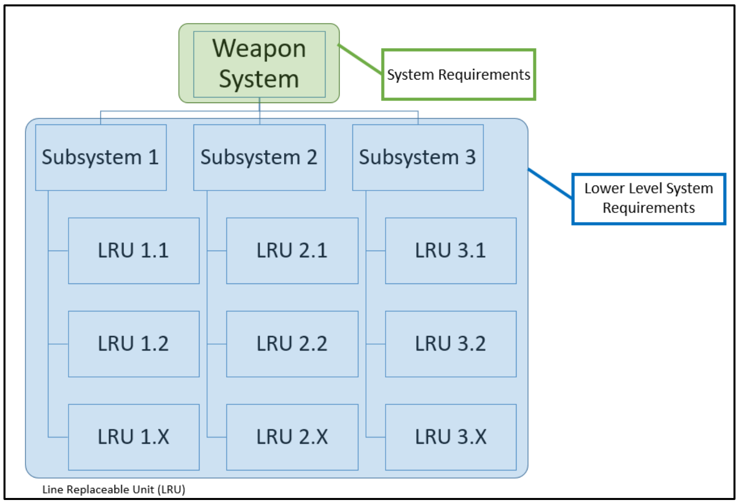


Figure A-4   Example Specification Tree

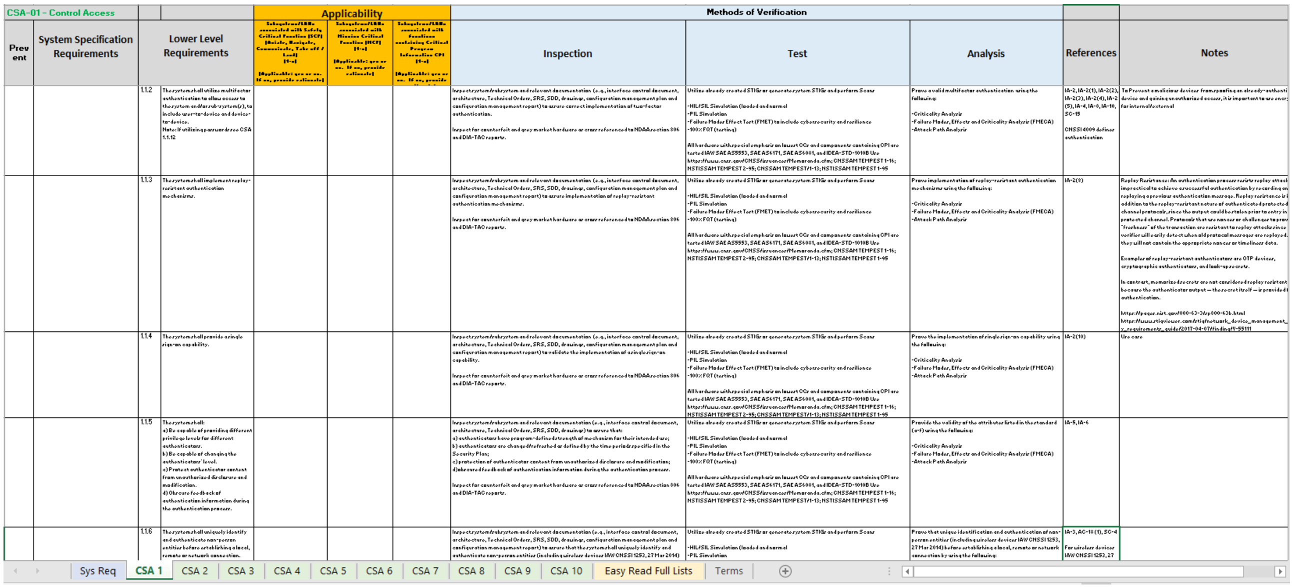
Table A-15 has decomposed SRD/System Specification requirements derived from the CSAs that should be put on contract, if applicable, for each MCF, SCF and functions associated with CPI. If not applicable, rationale shall be provided. These requirements are also tailorable. Tailorable means that requirements can be added as well. Also, refer to **Attachment 1** for more details on the requirements in this Table.

Table A-14 Derived SRD/System Specifications based on the CSA decomposition

KPP Pillars	SRD/System Specification Requirements
Prevent	**CSA-01 - Control Access**
1.1	The system shall ensure that only authenticated User-to-device and device-to-device entities are allowed access or interconnection to the system or sub-elements within its boundaries.
1.2	The system shall enforce least privilege access for authenticated persons and non-person entities necessary to accomplish assigned tasks.
Prevent	**CSA-02 - Reduce System's Cyber Detectability**
2.1	The system shall protect against adversary detection and exploitation of information leakage due to electromagnetic emanations.
2.2	The system shall minimize connections (wired/wireless) to meet mission requirements.
Prevent	**CSA-03 - Secure Transmissions and Communications**
3.1	The system shall implement data protection measures for information transmissions and communications in transit (per appropriate classification levels).
Prevent	**CSA-04 - Protect System's Information from Exploitation**
4.1	The system shall ensure information integrity and performance as validated and baselined.
4.2	The system shall protect data while at rest (per appropriate classification levels).
4.3	The system shall implement safeguards to deter, detect, prevent, and respond to software, hardware, and firmware tampering.
4.4	The system shall employ sanitization processes at the system, subsystem, and component levels.
Prevent	**CSA-05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels**
5.1	The system design shall partition "mission critical," "safety critical," and CPI functionality from less critical functions and segregate classified information.
5.2	The system shall ensure safety critical and mission critical functions are prioritized appropriately to ensure mission completion.
Prevent	**CSA-06 – Minimize and Harden Attack Surfaces**
6.1	The system shall provide the capability to configure external interfaces as required to perform safety critical and mission critical functions.
6.2	The system shall ensure interfaces capabilities maintain their mission effectiveness while under a cyberattack, while remaining accessible for safety/mission functionality.
Mitigate	**CSA-07 – Baseline & Monitor Systems and Detect Anomalies**
7.1	The system shall monitor operational parameters, boundaries, and configuration controls Prerequisite CSA 4.1
7.2	The system shall analyze performance through a baseline comparison to detect anomalies and attacks.
7.3	The system shall generate and store logs.
Mitigate	**CSA-08 - Manage System Performance if Degraded by Cyber Events**
8.1	The system shall alert Users of detected anomalies and attacks. Prerequisite: CSA 5, 7
8.2	The system shall provide capabilities to shed non-mission critical functions, systems/subsystems, and interfaces. Prerequisite: CSA 5, 7
8.3	The system shall maintain mission critical functions in a cyber-contested operational environment during/after observed anomaly(ies). Prerequisite: CSA 4, 5 & 7
8.4	The system shall maintain safety critical functions in a cyber-contested operational environment during/after observed anomaly(ies). Prerequisite: CSA 4, 5 & 7

KPP Pillars	SRD/System Specification Requirements
8.5	The system shall fail secure when mission critical functions are no longer operational in a contested environment. Prerequisite: CSA 4, 5 & 7
Recover	**CSA-09 - Recover System Capabilities**
9.1	The system shall provide the capability to recover to a known state in near real time.
P/M/R	**CSA-10 - Actively Manage System Configurations to Counter Vulnerabilities at Tactically Relevant Speeds**
10.1	The system shall have the capability to update scans to ensure appropriate, applicable requirements are captured (e.g. STIGS, SRG, etc.) for: (a) hardware (b) software (c) firmware
10.2	Actively manage System's Configurations to achieve and maintain an operationally relevant Cyber Survivability Risk Posture (CSRP)

Figure A-5 provides an example of how each MCF, SCF, and functions associated with CPI should be laid out to compare against each requirement from the SRD/System Specification language. A program will have 1-to-n Safety Critical Functions (e.g., aviate, navigate, communicate, take-off and land), the Mission Critical Functions, and the functions associated with CPI. The Table seen in Figure A-5 should be completed and the appropriate requirements from **Attachment 1** should be indicated as applicable for the individual SCF, MCF, and functions associated with CPI. All requirements are mapped from the NIST 800-53r5 where applicable.



CSA-01 – Control Access				Applicability			Methods of Verification				
Prevent	System Specification Requirements	Lower Level Requirements		Subsystems/LRUs associated with Safety Critical Function (SCF) (Aviate, Navigate, Communicate, Take off / Land) [1-n] [Applicable: yes or no. If no, provide rationale]	Subsystems/LRUs associated with Mission Critical Function (MCF) [1-n] [Applicable: yes or no. If no, provide rationale]	Subsystems/LRUs associated with functions containing Critical Program Information CPI [1-n] [Applicable: yes or no. If no, provide rationale]	Inspection	Test	Analysis	References	Notes
		1.1.2	The system shall utilize multifactor authentication to allow access to the system and/or sub-system(s), to include user-to-device and device-to-device. Note: If utilizing passwords see CSA 1.1.12				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to assure correct implementation of two-factor authentication. Inspect for counterfeit and grey market hardware or cross referenced to NDAA section 806 and DIA-TAC reports.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B Use https://www.cnss.gov/CNSS/issuances/Memoranda.cfm; CNSSAM TEMPEST 1-16; NSTISSAM TEMPEST 2-95; CNSSAM TEMPEST/1-13; NSTISSAM TEMPEST 1-95	Prove a valid multifactor authentication using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(5), IA-4, IA-8, IA-10, SC-15 CNSSI 4009 defines authentication	To Prevent a malicious devices from spoofing an already-authenti device and gaining unauthorized access, it is important to use encr for internal/external
		1.1.3	The system shall implement replay-resistant authentication mechanisms.				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to assure implementation of replay-resistant authentication mechanisms. Inspect for counterfeit and grey market hardware or cross referenced to NDAA section 806 and DIA-TAC reports.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B Use https://www.cnss.gov/CNSS/issuances/Memoranda.cfm; CNSSAM TEMPEST 1-16; NSTISSAM TEMPEST 2-95; CNSSAM TEMPEST/1-13; NSTISSAM TEMPEST 1-95	Prove implementation of replay-resistant authentication mechanisms using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2(8)	Replay Resistance: An authentication process resists replay attack impractical to achieve a successful authentication by recording an replaying a previous authentication message. Replay resistance is i addition to the replay-resistant nature of authenticated protected channel protocols, since the output could be stolen prior to entry in protected channel. Protocols that use nonces or challenges to prov "freshness" of the transaction are resistant to replay attacks since verifier will easily detect when old protocol messages are replayed. they will not contain the appropriate nonces or timeliness data. Examples of replay-resistant authenticators are OTP devices, cryptographic authenticators, and look-up secrets. In contrast, memorized secrets are not considered replay resistant because the authenticator output — the secret itself — is provided f authentication. https://pages.nist.gov/800-63-3/sp800-63b.html https://www.stigviewer.com/stig/network_device_management_y_requirements_guide/2017-04-07/finding/V-55111
		1.1.4	The system shall provide a single sign-on capability.				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to validate the implementation of a single sign-on capability. Inspect for counterfeit and grey market hardware or cross referenced to NDAA section 806 and DIA-TAC reports.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B Use https://www.cnss.gov/CNSS/issuances/Memoranda.cfm; CNSSAM TEMPEST 1-16; NSTISSAM TEMPEST 2-95; CNSSAM TEMPEST/1-13; NSTISSAM TEMPEST 1-95	Prove the implementation of single sign-on capability using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2(10)	Use care
		1.1.5	The system shall: a) Be capable of providing different privilege levels for different authenticators. b) Be capable of changing the authenticators' level. c) Protect authenticator content from unauthorized disclosure and modification. d) Obscure feedback of authentication information during the authentication process.				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings) to assure that: a) authenticators have program-defined strength of mechanism for their intended use; b) authenticators are changed/refreshed or defined by the time periods specified in the Security Plan; c) protection of authenticator content from unauthorized disclosure and modification; d) obscured feedback of authentication information during the authentication process. Inspect for counterfeit and grey market hardware or cross referenced to NDAA section 806 and DIA-TAC reports.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B Use https://www.cnss.gov/CNSS/issuances/Memoranda.cfm; CNSSAM TEMPEST 1-16; NSTISSAM TEMPEST 2-95; CNSSAM TEMPEST/1-13; NSTISSAM TEMPEST 1-95	Provide the validity of the attributes listed in the standard (a-f) using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-5, IA-6	
		1.1.6	The system shall uniquely identify and authenticate non-person entities before establishing a local, remote or network connection.				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to assure that the system shall uniquely identify and authenticate non-person entities (including wireless devices IAW CNSSI 1253, 27 Mar 2014)	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation	Prove that unique identification and authentication of non-person entities (including wireless devices IAW CNSSI 1253, 27 Mar 2014) before establishing a local, remote or network connection by using the following:	IA-3, AC-18 (1), SC-4 For wireless devices IAW CNSSI 1253, 27	

Figure A-5 Example of SRD/SSS to Prevent/Mitigate/Recover & CSAs

2.3. Statement of Objectives and Statement of Work

The PO is responsible for developing the Statement of Objectives (SOO) to identify the top-level objectives of a Government acquisition and/or procurement as outlined in the Request for Proposal (RFP). The SOO is then used by the contractor to develop a Statement of Work (SOW), Work Breakdown Structure (WBS), Integrated Program Management Report (IPMR) and other documents required by the RFP. Development of the SOO is not necessary if the PO can clearly identify the Government Requirements in a SOW. In some circumstances, the Government will develop a SOW instead of a SOO. Determining the use between the SOO and SOW should be documented in the Acquisition Strategy. Below are SOO/SOW paragraphs that are highly recommended for SSE requirements. If a Section is not used, the preparer should provide rationale to the Chief Engineer as to why the Section was not applicable prior to releasing the RFP. Tailoring of the language is also allowed, but also requires justification to the Chief Engineer prior to RFP release.

The following subsections shall be included on contract, but are tailorable, based on applicability. Tailorable also means that requirements can be added. Further details are available in **Attachment 2** addressing applicable DIDs for each CDRL, as well as, recommended delivery schedule. All SOO/SOW statements have been traced back to the corresponding CSA controls and NIST 800-53r5 controls, as **Attachment 3** pertains to.

NOTE: The CDRL numbers listed correspond to the numbers in the Table in **Attachment 2**.

2.3.1. Overall Systems Security Engineering

A. The contractor shall describe the planned Systems Security Engineering (SSE) approach to meet the technical activities of the contract and overall technical management of the program as part of the overall systems engineering process documented in the Systems Engineering Management Plan (SEMP). The contractor's SEMP shall align with the content of the Government Systems Engineering Plan (SEP) (CDRL 61).

B. The contractor shall derive all SSE requirements and put into specification(s) (CDRL 2, 3 and 13). Systems Security Engineering includes the following areas: Program Protection, Cybersecurity, Cyber Resiliency, Trusted Systems and Networks (TSN), Anti-Tamper, and Information Protection. The contractor shall trace and verify all SSE requirements through the Systems Engineering Processes, and document within the Requirements Traceability Verification Matrix (RTVM) (CDRL 11). Development contractors shall incorporate Anti-Tamper mitigations into system design and engineering and flow down requirements to sub-contractors. The contractor shall utilize modeling and simulations for verification of specifications where possible. The contractor shall accredit and verify modeling and simulation used for closure of any specification requirements in accordance with MIL-STD-3022 (CDRL 46 and 47).

C. C. The contractor shall utilize Digital Engineering for the derivation of Systems Security Engineering (SSE) requirements. Systems Security Engineering includes the following areas: Program Protection, Cybersecurity, Cyber Resiliency, TSN, Anti-Tamper (AT), and Information Protection (IP). The contractor shall trace and verify all SSE requirements through the Systems

Engineering Processes utilizing Digital Engineering practices, models and tools (CDRL 2, 3, 12 and 13). The Contractor shall use Model Based Systems Engineering/Digital Engineering (MBSE/DE) tools to design, develop, test, verify, certify, validate, and deliver the system for Cybersecurity and resiliency. The Contractor shall integrate the models and have a bi-directional tractability for any non-integrated models. The MBSE/DE shall be controlled through the Contractor's configuration control plan. The Contractor shall [deliver, provide access to] the MBSE/DE model(s) to the Government in its entirety with all native/source files to the lowest level and delivered for all major milestones and systems engineering technical reviews. The contractor shall provide access to the MBSE/DE models until final delivery of the models. The MBSE/DE model shall trace and store all requirements below. The models shall produce the products for the CDRLs/DIDs listed in the xx sections of the SOO/SOW. The contractor shall have rules in the models to help verify appropriate requirements have been derived and the design embodies the requirements appropriately.

> **NOTE:** Digital Engineering is in the infancy stage and this paragraph may not be required on contract, or can be tailored to highly encourage utilizing Digital Engineering practices, models and tools.

D. The contractor shall allocate system security and Cyber Resiliency requirements to architectural entities and system elements. The contractor shall trace system architecture design to the requirements derived from the agreed to Security Controls Traceability Matrix (SCTM) NIST 800-53r5 (or current revision) controls (Contractor Security Plan/Security Assessment Plan) IAW DoDI 8500.01 and DoDI 8510.01 and TSN per DoDI 5200.44, AT per DoDI 5200.39 and the Anti-Tamper Technical Implementation Guide (TIG), and Cyber Resiliency requirements. The contractor shall allocate requirements to the Safety Critical Functions (SCFs), Mission Critical Functions (MCFs), and functions associated with Critical Program Information (CPI) commensurate with operational-risk and acquisition-risk categorization. The contractor shall utilize the lower level requirements located in Attachment 1 of the USAF Systems Security Engineering Acquisition Guidebook, as applicable, and provide a requirements traceability verification matrix (CDRL 11). The contractor shall ensure integration and verification that SCFs, MCFs, and CPI have the appropriate segregation and diverse redundancy in the architecture entities and system elements to complete the mission (Cyber Resiliency), see requirement Section for more information. In addition, the Architect Design Document shall include architectural entities and system elements analysis of any other systems'/subsystems' interconnects/interfaces that are not SCF, MCF, or functions associated with CPI. If there are interconnects/interfaces, the Architect Design Document shall ensure the appropriate system segregation and diverse system redundancy is maintained for the SCF, MCF, and functions associated with CPI (CDRL 24).

E. A. The contractor shall develop a Test and Evaluation Program Plan that is aligned to the Government developed Test and Evaluation Master Plan (CDRL 5). The Government shall be able to participate in all cyber testing. In addition, the contractor shall allow the Government time in the laboratories and with the space and weapon system to conduct cyber testing (e.g. cooperative vulnerability and penetration assessment, adversarial assessment, etc.). The contractor shall conduct its own space and weapon system cyber testing (e.g. cooperative vulnerability and penetration assessment, adversarial assessment, etc.) and provide the test plan, procedures and reports (CDRLs 3, 4, 6, 7,8, 9, 48, and 49). The contractor shall deliver hardware and software System Integration Laboratory(ies) (SILs) for the Government to conduct cyber testing at PDR, CDR and update the SILs to the correct configuration of the program.

F. The contractor shall provide a SSE requirements implementation assessment per Appendix E of the DAF Systems Security Engineering Cyber Guidebook. In addition, the contractor shall provide courses of action with cost details to get all Systems Security Engineering risk below medium (CDRL 58).

G. The contractor shall perform a Program Protection (PP) / System Security Risk Assessment of the system per the Risk Management section in Appendix A: USAF System Security Engineering Acquisition Guidebook, utilizing the System Security Working Groups. These risks shall be part of the overall program risks and safety risks (CDRLs 14, 59 and 60).

H. The contractor shall participate in the Government-led IPTs or System Security Working Group (SSWG) [Quarterly, Monthly, 60 days prior to any System Engineering Technical Review (SETR), etc.] to provide technical input to the Government’s program protection planning and SSE activities (CDRLs 16 and 17).

2.3.2. Program Protection

A. The contractor shall deliver a Program Protection Implementation Plan (PPIP), CDRL 1, that is aligned to the Government developed Program Protection Plan (PPP). The contractor shall integrate the PPIP activities in the Integrated Master Plan/Integrated Master Schedule (IMP/IMS) (CDRL 10).

B. The Contractor shall create, maintain and operate a formal incident response and forensic capability for protection of Control Unclassified Information (CUI) residing on non-federal Information Systems. The Contractor shall include the subcontractors and suppliers that perform support work that involves CUI. The scope and extent of this incident response and forensic capability shall be consistent with the assigned Contractor’s Cyber Maturity Model Certification (CMMC) level (CDRL TBD).

C. The Contractor shall establish a System Security Plan (SSP) citing Cyber Incident Reporting (IR) requirements. Any IR that impacts a Contractor system under the contract's DFAR clauses and provisions must be reported within 72 hours of the suspected incident. To report cyber incidents, the Contractor must have a medium assurance certificate. A review must be conducted so that the scope of the compromise can be understood. At a minimum, this review must cover the information specified in DID xx and as cited in CDRL 19 and under NIST SP800-61 Rev. 2 guidelines. As a minimum, the CDRL 19 must provide IR review reporting to include, but not limited to: Identification of affected systems; Affected Users accounts; Affected data; and Other systems that might have been compromised.(CDRL 19)

D. The Contactor shall be prepared and report cyber incidents that result in an actual or potentially adverse effect on the covered contractor information system and/or Covered Defense Information (CDI) residing therein, or on a contractor's ability to provide operationally critical support. The Contractor shall report status of the incident-handling capability including plan-of-actions for capabilities not at full operational status, and periodic operational status. The Contractor shall provide status of a cyber-incident from first identification to closure as described in the Contractor incident-handling plan. The contractor shall report cyber incidents (for all Sections in the SOO/SOW) to the Government via CDRL/DID, IAW DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting", 48 CFR 252.204-7007 Compliance with Safeguarding Covered Defense Information Controls, 32 CFR 236.4. Cyber Incident Reporting Procedures and to the Defense Cyber Crime Center (DC3) via the DIBNet and Joint Deficiency Reporting System. (CDRL 15)

> **NOTE:** Guidance for assessing compliance and enhancing protections required by DFARS Clause 252.204-7302, Safeguarding Covered Defense Information and Cyber Incident Reporting, Policy can be found online at **https://www.acquisition.gov/ .**

E. The Contractor shall establish and document a digital forensics readiness plan, and upon an incident execute the plan on the covered information system to include the collection, examination, analysis, and reporting following practices described in NIST SP800-86, "Guide to Integrating Forensic Techniques into Incident Response", and NIST SP800-101 "Guidelines on Cell Phone Forensics". The contractor shall use a community-developed, standardized specification language for representing and exchanging information in the broadest possible range for cyber-investigation domains, including forensic science, incident response, and counter terrorism. The Contractor forensic team assessment as required shall initiate corrective actions to include securing identified vulnerabilities, improve existing security controls, and provide recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process. The Contractor shall follow practices described in NIST SP800-171 R2, "Protecting CUI in Non-Federal Systems and Organizations", and NIST SP800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" (CDRLs 62 and 63).

> **NOTE:** DIBNet is a web portal for sharing threat information between DoD and Defense Industrial Base (DIB) companies. CFR Part 236, DoD Defense Industrial Base Cybersecurity Activities.

F. The contractor shall conduct a Functional Thread Analysis (FTA) (CDRL 23) and Criticality Analysis. The contractor shall identify and document all internal and external system interfaces (CDRL 13). The contractor shall use the data from the FTA to inform an Attack Path Analysis. While conducting an Attack Path Analysis, the contractor shall identify and analyze the cyber-attack surface by listing any hardware, software, connection, data exchange, service, removable media, or any other system attribute that may expose it to exploitation and determine likely avenues of cyber-attack. The contractor shall perform a covert channel analysis to identify those aspects of communications within the space and weapon system that are potential avenues for covert storage and/or timing channels (CDRL 50).

2.3.3. Cybersecurity and Trusted Systems and Networks

> **NOTE:** Guidance for developing the Cybersecurity SOW Section is available in DAG (Chapters 6 & 9), AFI 17-101, and the DASD(SE)[16] and the DoD CIO website[17].

A. The contractor shall provide a Contractor Security Plan for the system (CDRL 19). The contractor shall provide a Security Assessment Plan (CDRL 29), a Security Assessment Report (CDRL 20), and a Plan of Action and Milestones (POA&M) (CDRL 54). The contractor shall ensure the weapons system's configuration has been baselined and documented to meet the cyber requirements (CDRL 55 and 56).

> **NOTE:** The Security Plan in CDRL 19 is the United States Air Force Contractor's Security Plan for Weapon Systems, and is not to be confused with the Security Plan used in RMF as delivered to the AO. The United States Air Force Contractor's Security Plan for Weapon Systems is the information required from the contractor in order for the Government to complete the Security Plan used in RMF.

B. The contractor shall provide the information required for the program office to obtain Interim Authority To Test (IATT) and Authority To Operate (ATO). The Contractor shall decompose the cyber certification requirements and flow into the specifications. (CDRL 41).

C. The contractor shall provide the Functional Thread Analysis to identify Safety Critical Functions, Mission Critical Functions, and functions associated with Critical Program Information (CPI) (for all CPI and Anti-Tamper (AT), see CPI/AT Section), IAW DoDI 5200.44, 5200.47, and 5000.39; Airworthiness Circular AC-17-01; and the USAF Combined Process Guide for CPI and Critical Component (CC) Identification (CDRL 23). In addition, the contractor shall ensure the Fault Tree Analysis (CDRL TBD) and Failure Modes Effects Analysis (FMEA) (CDRL 21) trace to the Criticality Analysis, which are documented in the Failure Modes Effects Criticality Analysis (FMECA) (CDRL 22). The contractor shall design the system with redundant/diverse redundant capability(ies) to reduce and eliminate single points of failure of all safety critical functions and mission critical functions based on risk.

> **NOTE:** For SMC, Airworthiness Circular AC-17-01 does not apply, the SMC Space Launch Readiness Review Process (SMC-G-1204) and SMC Space Flight Worthiness Criteria (SMC-G-1202) should be used instead.

[16] https://www.acq.osd.mil/se/initiatives/init_pp-sse.html
[17] http://dodcio.defense.gov/Library/

D. The contractor shall provide information to obtain a Defense Intelligence Agency – Threat Assessment Center (DIA-TAC) Report when Critical Components are known based on the Functional Thread Analysis. The contractor shall trace the Bill of Materials to the lowest critical components. The contractor shall update design via system engineering processes to ensure above-medium risk components are not in the system (CDRL 23).

E. The contractor shall ensure all hardware, with special emphasis on lowest critical components (CCs) and components containing CPI, are from trusted sources and are manufactured by approved personnel as documented in the contractor Security Plan. The contractor shall develop a Supply Chain Risk Management (SCRM) plan documented in the contractor Security Plan (CDRL 19), IAW the current version of CNSSD No. 505 and NIST SP800-161, to mitigate supply chain risk. The contractor shall ensure that no critical components procured are on the Section 806 (National Defense Authorization Act for FY 2011 (Public Law 111-383)) and Section 2339a (Title 10, United States Code) Lists in the Supplier Performance Risk System (SPRS) (CDRL 25, 27, 29). The contractor shall develop and implement a Counterfeit Parts Prevention Program (CDRL 26) in compliance with DFARS 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System, using SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B or similar practices to prevent the inclusion of counterfeit parts or parts with malicious logic. The contractor shall perform acceptance testing on lowest CCs and components containing CPI in accordance with the Counterfeit Parts Prevention Program (CDRL 29, 51, 52, and 53).

> **NOTE:** Contact the local Logistics functional for further sample language related to Supply Chain Risk Management (SCRM) that is more specific to each Air Force Acquisition Center. For example, AFLCMC/LG-LZ has a Product Support Contract Requirements Tool (PSCRT) with more specific sample language for SCRM.

F. The contractor shall provide a Software Development Plan (SDP) (CDRL 30) and the source code to complete software assurance independently for all safety critical functions, mission critical functions, and functions associated with CPI. The contractor shall design, develop and verify software per the SDP and the critical functions identified in the Functional Thread Analysis (CDRL 6,8, 29, and 33) The contractor's SDP shall include an analysis of any other systems that are not SCFs, MCFs, or functions associated with CPI, but are interconnected to such functions. If there are interconnects/interfaces, the software development plan shall ensure the software assurance is maintained for the SCF, MCF, and functions associated with CPI (CDRL 31, 32, 44, 55, 56 and 57).

G. The contractor shall develop an NSA-approved Key and Certificate Management Plan (KCMP) for each cryptographic system (CDRL 37). The contractor should obtain NSA Cyber and Crypto security certification requirements (IASRD, TSRD, TRANSEC and TEMPEST requirements). The contractor shall provide source data and analysis required to obtain NSA

Type-1 certification of the system. The cryptographic and Cybersecurity portions of the system design shall be reflected in the Contractor's Security Plan (CDRL 19).

> **NOTE:** Guidance for developing the NSA Cryptography SOW Section is available in the National Security Agency/Central Security Service (NSA/CSS) Policy Manual 1-52, CNSSI No. 4001, and AFMAN 17-1302-O.

H. The contractor shall provide the cables to complete TEMPEST testing for the Laboratories and Weapon System and Government access to the facilities to complete TEMPEST testing, source data, and analysis required to obtain TEMPEST certification of the system IAW NSTISSAM TEMPEST/1-92 and document their approach in the TEMPEST Control Plan (CDRL 38, 39 and 40).

> **NOTE:** Guidance for developing the TEMPEST SOW Section is defined in National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92 and AFMAN 17-1301. NSA TEMPEST certification program information can be found online[18].

2.3.4. Critical Program Information / Anti-Tamper

A. The contractor shall develop and implement Anti-Tamper (AT) protection measures to protect (by deterring, preventing, detecting, and/or reacting to anti-tamper attacks) the Government approved, Critical Program Information (CPI) per the DoD CPI Horizontal Protection Guidance (HPG), Anti-Tamper Technical Implementation Guide (TIG), and Anti-Tamper Desk Reference, and document in an AT Plan formatted IAW DoD ATEA Annex: Anti-Tamper Plan Template. The contractor shall trace the test plan requirement to the specification and verify through the systems engineering processes (CDRL 42 and 43).

> **NOTE:** The USAF AT Lead shall approve the AT plan prior to proposal release and continues to agree at major milestones and technical reviews.

2.3.5. Security Management / Information Protection

A. The contractor shall establish and maintain a security program to comply with requirements of the Government-provided Contract Security Classification Specification, DD Form 254, and other security related contractual requirements as indicated in all RFP/SOO/SOW documents.

[18] **https://apps.nsa.gov/iaarchive/programs/iad-initiatives/tempest.cfm**

B. The contractor shall apply Operations Security (OPSEC) in their management of the Program IAW AFI 10-701 Operations Security, the OPSEC Plan, and program's Critical Information List provided by the Government program office (CDRL 45).

C. The contractor shall provide OPSEC, Communications Security (COMSEC) and Cybersecurity (CS) training as part of its overall training requirements. OPSEC, COMSEC, and CS training outline specific actions to protect classified and sensitive unclassified information, activities and operations during the course of the contract.

> **NOTE:** Guidance for assessing compliance and enhancing protections required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting can be found online[19].

D. The contractor shall upon request:

(1) provide to the government, a System Security Plan (or extract thereof) and any associated plans of action developed to satisfy the adequate security requirements of DFARS 252.204-7012, and in accordance with NIST SP(SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" in effect at the time the solicitation is issued or as authorized by the contracting officer, to describe the contractor's unclassified information system(s)/network(s) where covered defense information associated with the execution and performance of this contract is processed, is stored, or transmits. System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System [Insert Contract Data Requirements List (CDRL)* Data Item Number Block 1 of DD Forum 1423-1].

(2) provide the government with access to the System Security Plan (or extracts thereof) and any associated plans of action for each of the Contractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), and the subcontractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), who process, store, or transmit covered defense information associated with the execution and performance of this contract. System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System [Insert Contract Data Requirements List (CDRL) Data Item Number Block 1 of DD Forum 1423-1].

> **NOTE:** A CDRL for System Security Plan (SSP) and Associated Plans of Action for a Contractor's Internal Unclassified Information System is found in Defense Pricing and

[19] **https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html**

Contracting Memo, Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, dated November 6, 2018. "(CDRL 18).

E. The contractor shall identify all covered defense information associated with the execution and performance of this contract. At the post-award conference the Contractor and the Government/Program Office shall identify and affirm marking requirements for all covered defense information, as prescribed by DoDM 5200.01 Vol 4, Controlled Unclassified Information, and DoDI 5230.24, Distribution Statements on Technical Documents, to be provided to the Contractor, and/or to be developed by the contractor, associated with the execution and performance of this contract. Track all covered defense information associated with the execution and performance of this contract. The Contractor shall document, maintain, and provide to the Government, a record of tier 1 level subcontractors, vendors, and/or suppliers who will receive or develop covered defense information – as defined in DFARS Clause 252.204-7012 and associated with the execution and performance of this contract (CDRL 18).

F. The contractor shall restrict unnecessary sharing and/or flow down of covered defense information associated with the execution and performance of this contract. The Contractor shall restrict unnecessary sharing and/or flow down of covered defense information – as defined in DFARS Clause 252.204-7012 and associated with the execution and performance of this contract – in accordance with marking and dissemination requirements specified in the contract and based on a 'need-to-know' to execute and perform the requirements of this contract. This shall be addressed and documented at the post-award conference (CDRL 18).

G. The Contractor shall flow down the requirements in paragraphs D.1 and D.2 to their tier 1 level subcontractors, vendors, and/or suppliers (CDRL 18).

H. The Contractor will notify the Government Contracting Activity and the Government Security Manager within 48 hours of any incident involving the actual or suspected compromise/loss of classified information to enable the Government to conduct immediate assessment of potential impact pending formal inquiry/investigation. Actual or suspected compromise of Covered Defense Information will be reported, IAW DFARS, Clause 252.204-7012 (CDRL 18).

I. The contractor shall develop and store all DoD technical data (e.g., source code) in a secure facility. The contractor shall prevent computer software, in the possession or control of non-DoD entities on non-DoD information systems, from having connections to the GIG through segregation control (e.g., firewall, isolated network, etc.) and document meeting this requirement in the contractor Security Plan (CDRL 18).

J. The contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required IAW the DISA Cloud Computing Security Requirements Guide (SRG)[20] unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer (DoD CIO) (CDRL 18).

NOTE: Guidance for developing the Cloud Computing SOW Section is available in DFARS Clause 252.239-7010 (Cloud Computing Services) and the DAG (Chapter 6).

NOTE: All deliveries should be annotated in the Integrated Master Plan (IMP) for the System Engineering Technical Reviews (Appendix A, Section 17.1).

3.0. Solicitation Documents

The Government, as part of the acquisition process, develops the following documents.

3.1. Request for Proposal – Contract Clauses and Provisions

An RFP is a solicitation used in negotiated[21] acquisition to communicate Government requirements to prospective contractors and to solicit proposals. The appropriate regulation clauses and provisions from the FAR, DFARS, and AFFARS will be selected and inserted into the RFP.

The clauses and provisions listed in this guidebook can be used as a reference for contract security language, but should be verified with the Procuring Contracting Officer (PCO) and applicable regulations, as they may not be required or applicable to be placed on certain types of contracts.

3.1.1. Recommended List of FAR Clauses and Provisions

FAR Subpart 4.4– Safeguarding Classified Information within Industry, provides guidance to the PCO for classified contracts. It describes security requirements, including use of DoDI 5220.22 CH-2 and DoDM 5220.22 Vol 2, for all contractors performing classified work under the National Industrial Security Program (NISP). It also mandates the use of a Contract Security Classification Specification, DD Form 254, by the PCO for all NISP classified contracts.

[20] DoD Cloud Computing Security Requirements Guide, Version 1, Release 3, 6 March 2017

[21] **https://www.acquisition.gov/content/part-15-contracting-negotiation**

The following FAR[22] clauses and provisions are recommended in AF contracts, when applicable:

1. ***52.204-2 Security Requirements (AUG 1996).***

   - Source: PART 52– Solicitation Provisions and Contract Clauses, and SUBPART 52.2– Text of Provisions and Clauses.
   - Rationale for Use: Clause applies to the extent that the contract involves access to information classified Confidential, Secret, or Top Secret. Clause requires the contractor to comply with the Department of Defense Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (NISPOM) for access to classified information. It requires the contractor to include clause in all subcontracts, if access to classified information is required.

2. ***52.204-21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2016).***
   - Source: PART 52– Solicitation Provisions and Contract Clauses, and SUBPART 52.2– Text of Provisions and Clauses.
   - Rationale for Use: This clause applies to information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. It does not include information provided by the Government to the public (such as on public Websites) or simple transactional information, such as necessary to process payments.

3. ***52.204-9 Personal Identity Verification of Contractor Personnel (JAN 2011).***
   - Source: PART 52– Solicitation Provisions and Contract Clauses, and SUBPART 52.2– Text of Provisions and Clauses.
   - Rationale for Use: Clause requires the contractor to comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication(FIPS) Number 201. It also requires the contractor to account for all forms of Government-provided identification issued to the contractor employees in connection with performance under this contract.

4. ***52.239-1 Privacy or Security Safeguards (AUG 1996).***
   - Source: PART 52– Solicitation Provisions and Contract Clauses, SUBPART 52.2– Text of Provisions and Clauses.
   - Rationale for Use: Clause requires contractor to not publish or disclose in any manner, without the PCO’s written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the Government. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the contractor shall afford the Government access to the contractor’s facilities, installations, technical capabilities, operations, documentation, records, and databases. It requires immediate notification if existing safeguards

[22] **https://www.acquisition.gov/**

have ceased to function and/or if either the Government or the contractor discovers new or unanticipated threats or hazards.

3.1.2. Recommended List of Defense FAR Supplement Clauses and Provisions

The following DFARS[23] clauses and provisions are recommended in AF contracts, when applicable.

- ***252.204-7000 Disclosure of Information (Oct 2016).***
  - Source: PART 204 – Administrative Matters, SUBPART 204.4 – Safeguarding Classified Information within Industry.
  - Rationale for Use*:* Clause prohibits the contractor from releasing any unclassified information, regardless of medium (e.g., film, tape, document) pertaining to any part of the contract or any program related to the contract, unless the Contracting Officer has given prior written approval or the information is otherwise in the public domain before the date of release.
- ***252.204-7003 Control of Government Personnel Work Product (Apr 1992).***
  - Source: PART 204 – Administrative Matters, SUBPART 204.4 – Safeguarding Classified Information within Industry.
  - Rational for Use: The contractor's procedures for protecting against unauthorized disclosure of information shall not require DoD employees or members of the Armed Forces to relinquish control of their work products, whether classified or not, to the contractor.

- ***252.204-7008 Compliance with Safeguarding Covered Defense Information Controls (OCT 2016).***
  - Source*:* PART 204 – Administrative Matters, SUBPART 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting.
  - Rationale for Use*:* Provision requires contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems by applying specified network security controls as identified in NISTSP800-171.

- ***252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (OCT 2019).***
  - Source*:* PART 204 – Administrative Matters, SUBPART 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting.
  - Rationale for Use*:* Clause is required for contractor services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.

- ***252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019).***
  - Source: PART 204 – Administrative Matters, SUBPART 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting.
  - Rational for Use: Clause requires a company to safeguard CDI, as defined in the clause, and to report to the DoD the possible exfiltration, manipulation, or other loss or compromise of unclassified CDI: or other activities that allow unauthorized access to the contractor's unclassified information system on which unclassified CDI is resident or transiting.

[23] **https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html**

- ***252.204—7019 Notice of NIST SP800-171 DoD Assessment Requirements***
  - Source: Part 204 – Administrative Matters, Subpart 204-73 - Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Rational for Use: Clause requires a Contractor to comply with NIST SP800-171 Assessment Requirements within three (3) years of the Contract Award date for their System Security Plan Architecture, Assessment cores and date by which the Assessment cited requirements are expected to be implemented

- ***252.204-7020 NIST SP800-171 DoD Assessment Requirements***
  - Source: Part 204 - Administrative Matters, Subpart 204-73 - Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Rationale for Use: This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171 in accordance with the Defense Federal Acquisition Regulation System (DFARS) clause at 252-204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting of this contract

- ***252.204-7501 Cybersecurity Maturity Model Certification (CMMC) level, policy***
  - Source: Part 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Rationale for Use: This clause requires that the Contracting Officer shall include in the solicitation the required CMMC level, if required by the requiring activity. Contracting Officers shall not award a contract, task order or delivery order to an Offeror that does not have a current (i.e. not more than 3 years old) CMMC certificate at the level required by the solicitation. Contractors are required to achieve, a time of award, a CMMC at the level specified in the solicitation. Contractors are required to maintain a current (i.e. not more than 3 years old) CMMC certificate at the specified level, if required by the Statement of Work or requirement document, throughout the life of the contract, task order or delivery order. Contracting Officers shall not exercise an option period or extend the period of performance on a contract, task order or delivery order, unless the contract has a current (i.e. not more than 3 years old) CMMC certificate at the level required by the contract, task order of delivery order. The CMMC assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary such as, but not limited to, when there are indications of issues with Cybersecurity and/or compliance with CMMC requirements

- ***252.208-74 Enterprise Software Agreements (Revised 30 OCT 2015).***
  - Source: PART 208 – Required Sources of Supplies and Services, SUBPART 208.74 – Enterprise Software Agreements.
  - Rationale for Use: Clause prescribes policy and procedures for acquisition of commercial software and software maintenance, including software and software maintenance that is acquired as part of a system or system upgrade, where practicable.[24]

[24] **http://www.esi.mil**

- ***252.209.7002 Disclosure of Ownership or Control by A Foreign Government (JUN 2010).***
  - <u>Source</u>*:* PART 209 – Contractor Qualifications, SUBPART 209.1 – Responsible Prospective Contractors.
  - <u>Rationale for Use</u>*:* Provision requires that under 10 U.S.C. 2536(a), no DoD contract under a national security program may be awarded to an entity controlled by a foreign Government if that entity requires access to proscribed information, i.e., Top Secret information, Communications security (COMSEC), Restricted Data (RD), Special Access Program (SAP), and Sensitive Compartmented Information (SCI), to perform the contract.

- ***252.211-7003 Item Unique Identification and Valuation (MAR 2016).***
  - <u>Source</u>*:* PART 211 – Describing Agency Needs, SUBPART 211.2 – Using and Maintaining Requirements Documents.
  - <u>Rationale for Use</u>*:* Clause requires marking items delivered to DoD with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items. These unique identifiers must be via a method that is in commercial use and has been recognized by DoD.

- ***252.225-7048 Export-Controlled Items (JUN 2013).***
  - <u>Source</u>: PART 225 — Foreign Acquisition, SUBPART 225.79 — Export Control.
  - <u>Rationale for Use</u>: Clause requires the contractor to comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State IAW the International Traffic in Arms Regulations (ITAR). The contractor shall consult with the Department of State regarding any questions relating to the compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the Export Administration Regulations (EAR). It requires inclusion in all subcontracts.

- ***252.225-7049 Prohibition on Acquisition of Commercial Satellite Services from Certain Foreign Entities—Representations (Jan 2018).***
  - <u>Source</u>: PART 225 – Foreign Acquisition, SUBPART 225.772-5 – Solicitation provision.
  - <u>Rationale for Use</u>: Provision indicates that the CO will not award a contract for commercial satellite services to a foreign entity (e.g., China, North Korea, terrorist state, etc.) without approval of the USD (A&S) and USD (R&E) or Under Secretary of Defense for Policy [USD (P)].

- ***252.239-7000 Protection Against Compromising Emanations (OCT 2019).***
  - <u>Source</u>: PART 239 – Acquisition of Information Technology, SUBPART 239.71 – Security and Privacy for Computer Systems.
  - <u>Rationale for Use</u>: Clause requires the contractor to use only information technology, as specified by the Government that has been accredited to meet the appropriate information assurance requirements of the National Security Agency National TEMPEST Standards. For acquisitions involving IT, that requires protection against compromising emanations. It requires the contractor to provide a TEMPEST accreditation date.

- ***252.239-7001 Information Assurance Contractor Training and Certification (JAN 2008).***
  - Source: PART 252 – Solicitation Provisions and Contract Clauses, SUBPART 252.204-7000 – Disclosure of Information.
  - Rationale for Use: Clause requires contractor personnel accessing information systems to have the proper and current information assurance certification to perform information assurance, IAW DoD 8570.01-M. It requires the Government to ensure that the certifications and certification status of all contractor personnel is identified, documented, and tracked.

- ***252.239-7009 Representation of Use of Cloud Computing (SEP 2015).***
  - Source*:* PART 239 – Acquisition of Information Technology, SUBPART 239.76 – Cloud Computing.
  - Rationale for Use*:* Provision requires the contractor to indicate whether the use of cloud computing is anticipated under the contract.

- ***252.239-7010 Cloud Computing Services (OCT 2016).***
  - Source: PART 239 – Acquisition of Information Technology, SUBPART 239.76 – Cloud Computing.
  - Rationale for Use: Clause is applicable when contractor is using cloud computing to provide information technology services in the performance of the contract. It requires the contractor to implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required IAW the Cloud Computing SRG. It also requires the contractor to report all cyber incidents related to the cloud computing service provided under the contract. Reports must be submitted to the Government via https://dibnet.dod.mil/portal/intranet/.

- ***252.239-7017 Notice of Supply Chain Risk (FEB 2019).***
  - Source: PART 239 – Acquisition of Information Technology, SUBPART 239.73 – Requirements for Information Relating to Supply Chain Risk.
  - Rationale for Use: Clause implements Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year 2011 (Pub. L. 111-383) and elements of DoDI 5200.44.

- ***252.239-7018 Supply Chain Risk (FEB 2019).***
  - Source: PART 239 – Acquisition of Information Technology, SUBPART 239.73 – Requirements for Information Relating to Supply Chain Risk.
  - Rationale for Use: Clause applies to the acquisition of commercial items, for IT, whether acquired as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, as defined by 239.7301. It defines "supply chain risk" as the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system. It requires the contractor to mitigate supply chain risk in the provision of supplies and services to the Government.

- ***252.246-7003 Notification of Potential Safety Issues (JUN 2013).***
  - Source: PART 246 – Quality Assurance, SUBPART 246.3 –Contract Clauses, SUBPART 246.371 – Notification of Potential Safety Issues.
  - Rationale for Use: Clause indicates contractors and their subcontractors will notify the Government of any nonconformance or defect for critical components identified as critical safety items. This means the nonconformance or defect could result in the loss of a weapon system or property damage

exceeding $1,000,000.00. For any critical components identified under this clause, the contractor would advise the Government within 72 hours of any performance issues which could result in mission compromise.

- ***252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System (AUG 2016).***
  - Source: PART 246 – Quality Assurance, SUBPART 246.8 – Contractor Liability for Loss of or Damage to Property of the Government, SUBPART 246.870 – contractor's Counterfeit Electronic Part Detection and Avoidance Systems.
  - Rationale for Use: Clause indicates contractors and their subcontractors that supply electronic parts or products that include electronic parts are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to do so may result in disapproval of the purchasing system by the PCO and/or withholding of payments.

- ***Software Assurance DFARS Clauses and Provisions***
  - Source: Section 5 of the Carnegie Mellon University Software Engineering Institute CMU/SEI-2018-SR-025, "Program Manager's Guidebook for Software Assurance", Dec 2018
    - *252.227-7013* Rights in Technical Data--Noncommercial Items (FEB 2014)
    - *252.227-7014* Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (FEB 2014)
    - *252.227-7015* Technical Data–Commercial Items (FEB 2014)
    - *252.227-7016* Rights in Bid or Proposal Information (JAN 2011)
    - *252.227-7017* Identification and Assertion of Use, Release, or Disclosure Restrictions (JAN 2011)
    - *252.227-7019* Validation of Asserted Restrictions--Computer Software (SEP 2016)
    - *252.227-7028* Technical Data or Computer Software Previously Delivered to the Government (JUN 1995)
    - *252.227-7030* Technical Data--Withholding of Payment (MAR 2000)
    - *252.227-7037* Validation of Restrictive Markings on Technical Data (SEP 2016)
  - Rationale for Use: These DFARS clauses and provisions are recommended as part of a software assurance strategy that ensures the Government obtains unlimited Government-purpose rights to all the data associated with computer software. Through this, the Government can then independently reproduce, recreate, or recompile the delivered source code to independently validate that the contractor has met the contract deliverable requirements. Without these rights, the program office would also be unable to fix vulnerabilities and reduce security risks to the program throughout the program's life cycle.

3.1.3. Recommended List of Air Force FAR Supplement Clauses and Provisions

The following Air Force FAR Supplement (AFFARS)[25] clauses and provisions are recommended in all AF contracts, where applicable.

[25] https://www.acquisition.gov/affars/solicitation-provisions-and-contract-clauses

1. **5352.204-9000 Notification of Government Security Activity and Visitor Group Security Agreements *(Oct 2017).***
   - Source: PART 5352 – Solicitation Provisions and Contract Clauses, SUBPART 5352.2 – Text of Provisions and Clauses.
   - Rationale for Use: Clause requires that the contract contain a DD Form 254 and VGSAs to perform at a Government location in the U.S. or overseas. Prior to beginning operations involving classified information on an installation identified on the DD Form 254, the contractor shall enter into a Visitor Group Security Agreement (or understanding) with the installation commander to ensure that the contractor's security procedures are properly integrated with those of the installation. As a minimum, the agreement shall identify the security actions that will be performed. This requirement is in addition to visit request procedures contained in DoDI 5220.22 CH-2, National Industrial Security Program Operating Manual (NISPOM).

2. ***5352.215-9000 Facility Clearance (MAY 1996).***
   - Source: PART 5352 – Solicitation Provisions and Contract Clauses, SUBPART 5352.2 – Text of Provisions and Clauses.
   - Rationale for Use: Clause requires the contractor to possess, or acquire, prior to award of contract, a facility clearance equal to the highest classification stated on the Contract Security Classification Specification (DD Form 254).

3. ***5352.242-9000 Contractor Access to Air Force Installations (NOV 2012).***
   - Source: PART 5352 – Solicitation Provisions and Contract Clauses, SUBPART 5352.2 – Text of Provisions and Clauses.
   - Rationale for Use: Clause requires the contractor to submit a written request to the CO listing the following: contract number, location of work site, start and stop dates, and names of employees and subcontractor employees needing access to the base. It requires contractors to obtain base identification and vehicle passes for those who perform work on AF installation(s).

4. ***5352.242-9001 Common Access Cards (CACs) for Contractor Personnel (NOV 2012).***
   - Source: PART 5352 – Solicitation Provisions and Contract Clauses, SUBPART 5352.2 – Text of Provisions and Clauses.
   - Rationale for Use: Clause requires contractors and subcontractors to obtain CACs for logical access to unclassified or classified DoD computer networks and systems and/or for installation entry control or physical access to facilities and buildings. It requires contractor to provide a listing of personnel who require a CAC to the CO and return CACs within seven working days after termination, contract completion, or transfer.

3.2. Request for Proposal – Section L

Section L of the RFP provides instructions for the Offeror to prepare the proposal. The development of Section L is led by Contracts, but is a collaborative effort across multiple Functionals and the User. Section L instructs the Offeror on what must be delivered as part of the proposal. Section L specifically informs the Offeror how to construct the proposal, and requests the information to be evaluated IAW Section M. An RFP matrix will map Section M evaluation criteria, Section L requests for information and the related requirements, as applicable.

The focus of this Section herein is to provide a specific example of Program Protection / System Security Engineering (PP/SSE) sub-factor, which could be found in Section L. Refer to the AFLCMC Engineering

Guide to Writing RFP Technical Content[26] for more information on Sections L and M (Chapter 8: Section L and Chapter 9: Section M). The PP/SSE sub-factor replaces the Information Assurance (IA) sub-factor.

The following (tailorable) language should be included in all RFPs for acquisitions in which there is a requirement for the contractor to provide Program Protection/Systems Security Engineering, including Cybersecurity and Cyber Resiliency:

The Offeror shall describe, in a detailed narrative, the proposed plan for establishing Program Protection/Systems Security Engineering (PP/SSE) to include Cybersecurity and Cyber Resiliency processes within the System Engineering and Development processes as required by the <Insert appropriate requirements document(s): Statement of Objective (SOO) | Statement of Work (SOW) | Systems Requirement Document (SRD) | Specification (Spec)>.

The Offeror's narrative shall include:

1. The Offeror's strategy to achieve space and

2. weapon system Cyber Resiliency. This strategy utilizes the contractor Security Plan / Security Assessment Plan (SP/SAP), Architecture, and a Security Assessment Report to integrate Cybersecurity requirements into the System Specification (through the National Institute of Standards and Technology (NIST) 800-53r5 controls per DoDI 8500.01 and DoDI 8510.01).

3. Cyber Resiliency techniques and approaches as required by the SOO/SOW, SRD/Spec, SP/SAP, and Architecture.

4. A description of the Anti-Tamper (AT) Concept Plan in accordance with DoDI 5200.39 and DoDD 5200.47E.

5. Information Protection as required by the DD Form 254 and Security Classification Guide.

6. Integrated Master Plan (IMP) / Integrated Program Management Report (IPMR) identifying key events for compliance with the PP/SSE requirements as required by the SOO/SOW, SRD/Spec, and SP/SAP.

7. Design Approach: The Offeror shall provide a description of their technical approach for meeting the PP/SSE requirements stated in the SOO/SOW, SRD/Spec, and SP/SAP.

[26] https://cs2.eis.af.mil/sites/23230/RFPResource/SitePages/Home.aspx

3.3. Request for Proposal – Section M

The development of Section M is led by Contracts, but is a collaborative effort across multiple Functionals and the User. Section M in the RFP defines the factors, sub factors, and elements used to "grade" the Offeror's proposal.

The following (tailorable) language should be included in all RFPs for acquisitions in which there is a requirement for the contractor to provide Program Protection, including Cybersecurity and Cyber Resiliency:

Measure of Merit: *This sub-factor is met when the Offeror:*

Proposes a sound plan for Program Protection / Systems Security Engineering (PP/SSE) in accordance with Section L, paragraph <Insert the Section L paragraph that outlines all the instructions for what Offerors are to submit in response to the PP/SSE requirements (see par.3.2 herein)>*.*

3.4. Request for Proposal – Cost Volume - SSE Cost Estimate – Section B

The Cost Volume is part of Section B of the RFP. It is prepared by the Offeror and presents all costs, including the basis of estimate, implementation plan, and schedule. The RFP cost estimate for SSE is based on the SSE requirements outlined in the PPP or other SE documentation that define SSE requirements. AT related material used in the preliminary proposed design may be classified. The PO may provide the Offeror with instructions regarding inclusion of SSE considerations in the Cost Volume as follows:

The Offeror shall provide a complete detailed cost in the formal cost proposal and a CWBS for <Insert SYSTEM NAME> SSE engineering and architecture integration in the overall <Insert SYSTEM NAME> WBS. At a minimum, the contractor shall:

1. Indicate/estimate the design, engineering, development, testing, and other costs relative to SSE activities (e.g., CPI/CC identification, CA, vulnerability assessment, countermeasure development, counterfeit parts and firmware testing, etc.).

2. Indicate/estimate all costs associated with an SSE measure to include: (i) the cost to acquire, develop, integrate, operate, and sustain the measure over the system life cycle; (ii) the cost as a measure of impact to system performance; (iii) the cost of documentation and training; and (iv) the cost of obtaining evidence and conducting analysis necessary for SSE-related requirements.

3. Identify how the Offeror will account for Non-Recurring Engineering (NRE) costs associated with SSE requirements.

4. Describe the Offeror's approach to using projected cost-benefit tradeoffs in SSE countermeasure selection.

DOD ATEA Recommended AT Cost Estimate Language.

The DoD ATEA recommends specific AT cost estimate language. This language can be found in the DoD Anti-Tamper Desk Reference, Second Edition, April 2017 or by contacting the DoD ATEA via their website[27].

4.0. Government Acquisition Activities

The Government, as part of the acquisition process, conducts the following activities.

4.1. Systems Engineering Technical Reviews / Integrated Master Plan

SETRs provide PMs with formal assessments of a program’s technical health and maturity at key points in the development life cycle. SETRs evaluate whether required SE and SSE tasks have been completed before proceeding beyond critical events.

“Baking in” SSE

To attain the goal of “baking in” SSE into our acquisition process, programs must perform many SSE tasks early in the acquisition cycle. For this reason, entry criteria for the ASR is extensive. Programs that do not plan to conduct an ASR must ensure that the ASR entry criteria are accomplished prior to EMD contract award.

The following paragraphs provide suggested technical review entry criteria related to SSE for 10 Technical Reviews (9 primary Technical Reviews plus TRR). There are no unique SSE exit criteria beyond the delivery of meeting minutes and closure of critical action items. The entry criteria are organized into the following SSE threads that map to standardized SSE SOO/SOW language described in Section 2.3 of this Appendix:

Section 2.3.1	**Overall Systems Security Engineering.**
Section 2.3.2	**Program Protection.**
Section 2.3.3	**Cybersecurity and Trusted Systems and Networks.**
Section 2.3.4	**Critical Program Information (CPI) / Anti-Tamper (AT).**
Section 2.3.5	**Security Management / Information Protection.**

These SETR entrance and exit criteria should be included in the IMP in the contract.

Large acquisition programs, such as MDAPs, may require Independent Review Team (IRT) composition from separate U.S. Government organizations, whereas smaller acquisition programs may be able to structure an independent team from within the organization.

[27] https://at.dod.mil

Ideally, the IRT is consistent throughout the program life cycle and serves as a trusted technical advisor to the Component Acquisition Executive (CAE).

The IRT will identify and document critical issues that jeopardize achieving program or mission objectives, to include recommended corrective action. Results will be provided directly to the CAE, with coordination but not undue influence from the Program Managers Office. The PM, with support from the LSE, will review, develop, and implement corrective action to the satisfaction of the CAE. OUSD(R&E) will monitor the implementation of the independent review process. These IRT reviews are separate from the contractor TRR, but must be a part of the SEP workflow process.

4.1.1. Alternative Systems Review or EMD Contract Award

ENTRY CRITERIA for Overall SSE	SOO/SOW
All SSE requirements (Cybersecurity, TSN, CPI/AT, SCRM, V&V Testing, DD Form 254, DFARS) are adequately articulated in the EMD RFP (contract clauses, SRD, SOO/SOW).	N/A - USG Task
SSE is reflected in program planning documents [e.g., SEP, TEMP, RMP, Lifecycle Sustainment Plan (LCSP)].	N/A - USG Task
System architecture, developed utilizing CA, MCFs, SCFs, and mitigations to SSE risks, agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP), and included as in the CS/CSP/SP.	Section 2.3.1.D
SSE risks developed IAW the SSECG reviewed in conjunction with programmatic risks.	Section 2.3.1 G

ENTRY CRITERIA for Program Protection	SOO/SOW
PPP, developed IAW DoD Outline & Guidance, approved by Milestone Decision Authority (MDA) IAW DoDI 5000.85.	Section 2.3.2

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, approved by the Authorizing Official (AO).	Section 2.3.3 A
Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	Section 2.3.3 A
Results of Criticality Analysis (CA), conducted IAW DAG CH 9-3.1.3.1, reviewed and documented in the PPP.	Section 2.3.2 C
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic-Bearing Components (LBC) submitted to DIA TAC.	Section 2.3.3 E
Supply Chain Risk Management (SCRM) – Plans to ensure trusted manufacturing sources for critical HW and SW identified by the CA are documented in PPP and reflected in the EMD SOW and contract clauses.	Section 2.3.3 E
Software Assurance (SwA) - SwA requirements for software CCs from the CA are documented in the PPP and reflected in the EMD SOW.	Section 2.3.3 F

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
AT Concept Plan, developed IAW USAF AT Lead guidance, approved by USAF AT Lead and Program Executive Officer (PEO).	**Section 2.3.4 A**
CPI, developed IAW the USAF Process Guide For Critical Program Information (CPI) and Critical Component (CC) Identification identified, approved by the PEO, and listed in the PPP.	N/A - USG Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.2. Systems Requirements Review

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., System Spec, SEMP, TEPP, RTVM, RMP, and Digital Engineering models/tools/source data).	**Section 2.3.1 A,B,C,E,G,H**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
Top-level system architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	**Section 2.3.1.D**
SSE risks developed IAW the SSECG, updated and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and SSE Requirements Implementation Assessment developed per Appendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., concept PPIP and cyber incidents)	**Section 2.3.2** A,B
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.02, Table 2.	**Section 2.3.2**

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, reviewed and any changes approved by the Authorizing Official (AO).	**Section 2.3.3 A**
Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	**Section 2.3.3 A**
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**
Hardware Assurance (HwA) – Critical Components (CC) from CA containing Logic-Bearing Components (LBC) updated & submitted to DIA TAC.	**Section 2.3.3 E**
Supply Chain Risk Management (SCRM) – Plans to ensure trusted manufacturing sources for critical HW and SW identified by the FTA are documented in PPP and reflected in the EMD SOW and contract clauses.	**Section 2.3.3 E**
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP & PPP. SwA requirements are based on the FTA.	**Section 2.3.3 F**

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
AT Concept Plan, developed IAW USAF AT Lead guidance, reviewed and, any changes have been approved by USAF AT Lead and PEO	**Section 2.3.4 A**
CPI, developed IAW the USAF Process Guide For Critical Program Information (CPI) and Critical Component (CC) Identification identified, reviewed, and any changes approved by the PEO, and listed in the PPP.	N/A - USG Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.3. System Functional Review

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., System Spec, Allocated specs (HW & SW), SEMP, TEPP, RMP, and Digital Engineering models/tools/source data).	Section 2.3.1 A,B,C,E,G,H
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
Top-level system architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.1.D
SSE risks developed IAW the SSECG, updated and reviewed in conjunction with programmatic risks.	Section 2.3.1 G
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from SRR updated, including lower-level requirements per Appendix E.	Section 2.3.1 F

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., concept PPIP and cyber incidents)	Section 2.3.2 A,B
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.85.	Section 2.3.2

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems &Networks	SOO/SOW
Updated Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, reviewed and any changes approved by the Authorizing Official (AO).	Section 2.3.3 A
Updated Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	Section 2.3.3 A
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2 C
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic-Bearing Components (LBC) updated and submitted to DIA TAC.	Section 2.3.3 E
Supply Chain Risk Management (SCRM) – Plans to ensure trusted manufacturing sources for critical HW and SW identified by the FTA are documented in PPP and reflected in the EMD SOW and contract clauses.	Section 2.3.3 E
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP & PPP. SwA requirements are based on the FTA.	Section 2.3.3 F

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
AT Concept Plan, developed IAW USAF AT Lead guidance, reviewed and any changes have been approved by USAF AT Lead and Program Executive Officer (PEO).	Section 2.3.4 A
CPI, developed IAW the USAF Process Guide For Critical Program Information (CPI) and Critical Component (CC) Identification identified, reviewed and any changes approved by the PEO, and listed in the PPP.	N/A - USG Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.4. Preliminary Design Review

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., System Spec, Allocated specs (HW& SW), Subsystems Spec and CI specs, SEMP, TEPP, RMP, and Digital engineering Models/tools/source data).	**Section 2.3.1 A,B,C,E,G,H**
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Requirements Traceability Verification Matrix).	**Section 2.3.1 E**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
Detailed system architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	**Section 2.3.1.D**
SSE risks developed IAW the SSECG, updated, and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from SFR updated to include the component level assessment per Appendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., initial PPIP and cyber incidents)	**Section 2.3.2** A,B
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.02, Table 2.	**Section 2.3.2**

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Updated Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, reviewed, and any changes approved by the Authorizing Official (AO).	**Section 2.3.3 A**
Updated Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	**Section 2.3.3 A**
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic-Bearing Components (LBC) updated and submitted to DIA TAC.	**Section 2.3.3 E**
Supply Chain Risk Management (SCRM) – Plans to ensure trusted manufacturing sources for critical HW and SW identified by the FTA are documented in PPP and reflected in the EMD SOW and contract clauses.	**Section 2.3.3 E**
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP & PPP. SwA requirements are based on the FTA.	**Section 2.3.3 F**
An initial attack path analysis is completed and approved.	**Section 2.3.2 C**
Modeling and simulation accreditation and verification & validation plan completed and approved.	**Section 2.3.1 B**
Configuration Management Plan completed and approved.	**Section 2.3.3 A**
Initial Configuration Management Report completed and approved.	**Section 2.3.3 A**

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
Draft AT Plan, developed IAW USAF AT Lead guidance, reviewed and any changes have been approved by USAF AT Lead and Program Executive Officer (PEO).	**Section 2.3.4 A**
Draft Anti-Tamper Evaluation Plan (ATEP), developed IAW USAF AT Lead guidance, reviewed.	**Section 2.3.4 A**
CPI, developed IAW the USAF Process Guide For Critical Program Information (CPI) and Critical Component (CC) Identification identified, reviewed and any changes approved by the PEO, and listed in the PPP.	N/A - USG Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.5. Critical Design Review (CDR)

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., System Spec, Allocated specs (HW & SW), Subsystems Spec and CI specs, RMP, SEMP, TEPP, and Digital engineering Models/tools/source data).	**Section 2.3.1 A,B,C,E,G,H**
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Requirements Traceability Verification Matrix).	**Section 2.3.1 E**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
Final system architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	**Section 2.3.1.D**
SSE risks developed IAW the SSECG, updated and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from PDR updated per Appendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., final PPIP and cyber incidents)	Section 2.3.2 A,B
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.2, Table 2.	**Section 2.3.2**

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Updated Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, reviewed and any changes approved by the Authorizing Official (AO).	**Section 2.3.3 A**
Updated Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	**Section 2.3.3 A**
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic-Bearing Components (LBC) updated and submitted to DIA TAC.	**Section 2.3.3 E**
Supply Chain Risk Management (SCRM) – Plans to ensure trusted manufacturing sources for critical HW and SW identified by the FTA are documented in PPP and reflected in the EMD SOW and contract clauses.	**Section 2.3.3 E**
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP & PPP. SwA requirements are based on the FTA.	**Section 2.3.3 F**
TEMPEST control plan reviewed.	**Section 2.3.3 H**
Modeling and simulation accreditation and verification & validation report completed and approved.	**Section 2.3.1 B**
An updated attack path analysis is completed and approved.	**Section 2.3.2 C**
Final Configuration Management Report completed and approved.	**Section 2.3.3 A**

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
Final AT Plan, developed IAW USAF AT Lead guidance, reviewed and any changes have been approved by USAF AT Lead and Program Executive Officer (PEO).	**Section 2.3.4 A**
Final Anti-Tamper Evaluation Plan (ATEP), developed IAW USAF AT Lead guidance, approved by USAF AT Lead and Program Executive Officer (PEO).	**Section 2.3.4 A**
Initial Anti-Tamper Evaluation Report (ATER), developed IAW USAF AT Lead guidance, reviewed.	**Section 2.3.4 A**
CPI, developed IAW the USAF Process Guide For Critical Program Information (CPI) and Critical Component (CC) Identification identified, reviewed and any changes have been approved by the PEO, and listed in the PPP.	N/A - USG Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.6. Test Readiness Review (TRR)

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., Digital engineering Models/tools/source data).	**Section 2.3.1 C**
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Requirements Traceability Verification Matrix).	**Section 2.3.1.E**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
System architecture, updated as required, developed utilizing the FTA and mitigations to SSE risks, reviewed and agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	**Section 2.3.1.D**
SSE risks developed IAW the SSECG, updated, and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from CDR updated per Appendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., PPIP and cyber incidents)	Section 2.3.2 A,B

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	**Section 2.3.3 A**
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**
TEMPEST control plan reviewed.	**Section 2.3.3 H**

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
No TRR entry criteria.	N/A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.7. Functional Configuration Audit (FCA)

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., Digital engineering Models/tools/source data).	Section 2.3.1 C
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Requirements Traceability Verification Matrix).	Section 2.3.1 E
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
System architecture, updated as required, developed utilizing the FTA and mitigations to SSE risks, reviewed and agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.1.D
SSE risks developed IAW the SSECG, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1 G
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from TRR updated per Appendix E.	Section 2.3.1 F

ENTRY CRITERIA for Program Protection	SOO/SOW
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.02, Table 2.	Section 2.3.2

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, reviewed, and any changes approved by the Authorizing Official (AO).	Section 2.3.3 A
Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	Section 2.3.3 A
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2 C
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP & PPP. SwA requirements are based on the FTA.	Section 2.3.3 F
TEMPEST control plan reviewed.	Section 2.3.3 H
A subsystem attack path analysis is finalized and approved.	Section 2.3.2 C
Updated and finalized Configuration Management Report completed and approved.	Section 2.3.3 A

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
No FCA entry criteria.	N/A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.8. System Verification Review (SVR)

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g. Digital engineering Models/tools/source data).	**Section 2.3.1 C**
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, test reports, and Requirements Traceability Verification Matrix).	**Section 2.3.1 E**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A -USG Task
System architecture, updated as required, developed utilizing the FTA and mitigations to SSE risks, reviewed and agreed to by the AO, TSN, USAF AT Lead, and Information Protection (IP) and included as in the CS/CSP/SP.	**Section 2.3.1.D**
SSE risks developed IAW the SSECG, updated, and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from FCA updated per Appendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., PPIP and cyber incidents)	Section 2.3.2 A,B
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.85.	**Section 2.3.2**

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP800-18, reviewed, and any changes approved by the Authorizing Official (AO).	**Section 2.3.3 A**
Security Assessment Plan (SAP), developed IAW NIST SP800-53A, reviewed.	**Section 2.3.3 A**
Security Assessment Report (SAR), developed IAW NIST SP800-53A, App G, reviewed.	**Section 2.3.3 A**
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP & PPP. SwA requirements are based on the FTA.	**Section 2.3.3 F**
TEMPEST control plan reviewed.	**Section 2.3.3 H**
An attack path analysis is finalized and approved.	**Section 2.3.2 C**
Updated and finalized Configuration Management Report completed and approved.	**Section 2.3.3 A**

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
Anti-Tamper Evaluation Report (ATER), developed IAW USAF AT Lead guidance, reviewed.	**Section 2.3.4 A**

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.9. Production Readiness Review (PRR)

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., Digital engineering Models/tools/source data).	**Section 2.3.1 C**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
SSE risks developed IAW the SSECG, updated, and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from SVR updated per Appendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., PPIP and cyber incidents)	Section 2.3.2 A,B
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.02, Table 2.	**Section 2.3.2**

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
No PRR entry criteria.	N/A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

4.1.10. Physical Configuration Audit (PCA)

ENTRY CRITERIA for Overall SSE	SOO/SOW
SSE CDRL submittals reviewed (e.g., Digital engineering Models/tools/source data).	**Section 2.3.1 C**
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A - USG Task
SSE risks developed IAW the SSECG, updated, and reviewed in conjunction with programmatic risks.	**Section 2.3.1 G**
SSE Requirements Implementation Assessment CDRL reviewed and the assessment PRR updated perAppendix E.	**Section 2.3.1 F**

ENTRY CRITERIA for Program Protection	SOO/SOW
Program Protection CDRL submittals reviewed (e.g., PPIP and cyber incidents)	**Section 2.3.2 A,B**
PPP, developed IAW DoD Outline & Guidance, reviewed, updated as required, and approved by Milestone Decision Authority (MDA) IAW DoDI 5000.85, Table 2.	**Section 2.3.2**

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, & Trusted Systems & Networks	SOO/SOW
PPP Criticality Analysis (CA) Appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	**Section 2.3.2 C**

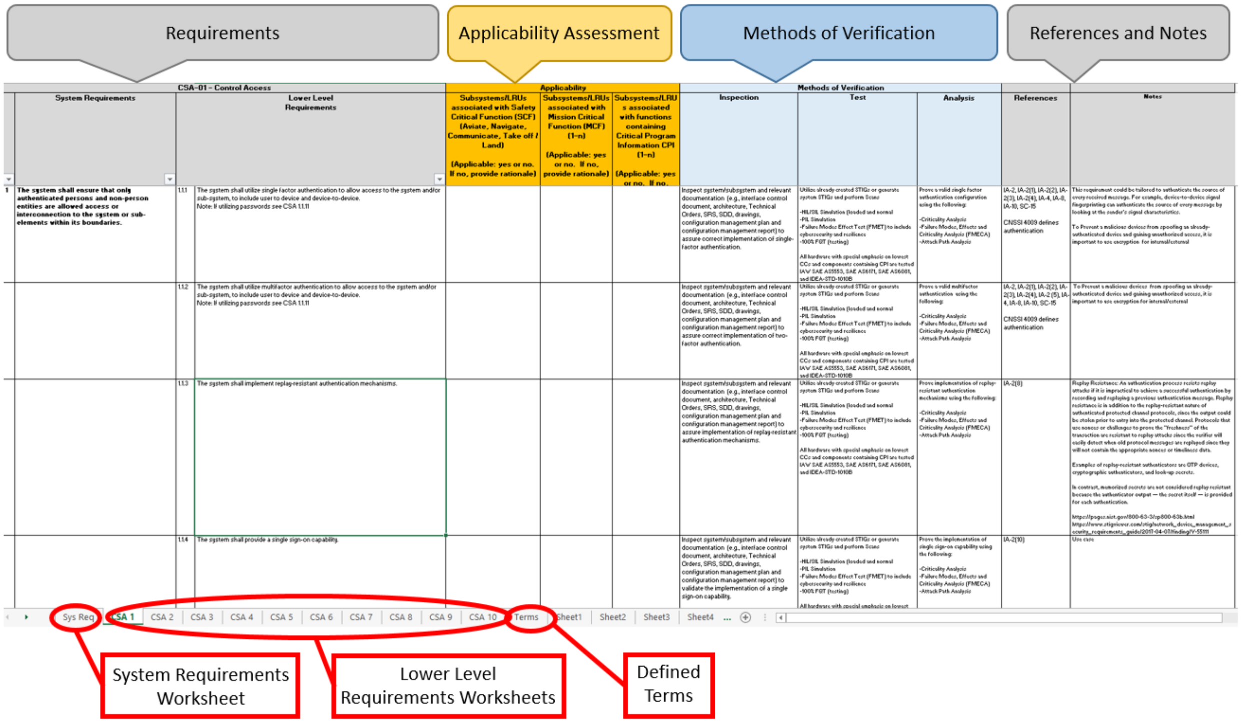
ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
No PCA entry criteria.	N/A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DoDI 5200.48, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A - USG Task

Attachment 1
Cybersecurity and Cyber Resiliency System & Lower Level Specification Requirements

Cybersecurity and
Cyber Resiliency Sys

The “Cybersecurity and Cyber Resiliency System and Lower Level Specification Requirements” Excel workbook embedded above contains a worksheet for system-level requirements, as well as, multiple worksheets for the lower-level system requirements (Figure A-6) intended for the engineers experienced in DoD acquisitions.



CSA-01 - Control Access				Applicability			Methods of Verification				
	System Requirements		Lower Level Requirements	Subsystems/LRUs associated with Safety Critical Function (SCF) (Aviate, Navigate, Communicate, Take off / Land) (Applicable: yes or no. If no, provide rationale)	Subsystems/LRUs associated with Mission Critical Function (MCF) (1-n) (Applicable: yes or no. If no, provide rationale)	Subsystems/LRUs associated with functions containing Critical Program Information CPI (1-n) (Applicable: yes or no. If no,	Inspection	Test	Analysis	References	Notes
1	The system shall ensure that only authenticated persons and non-person entities are allowed access or interconnection to the system or sub-elements within its boundaries.	1.1.1	The system shall utilize single factor authentication to allow access to the system and/or sub-system, to include user to device and device-to-device. Note: If utilizing passwords see CSA 1.1.11				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to assure correct implementation of single-factor authentication.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B	Prove a valid single factor authentication configuration using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-4, IA-8, IA-10, SC-15 CNSSI 4009 defines authentication	This requirement could be tailored to authenticate the source of every received message. For example, device-to-device signal fingerprinting can authenticate the source of every message by looking at the sender's signal characteristics. To Prevent a malicious devices from spoofing an already-authenticated device and gaining unauthorized access, it is important to use encryption for internal/external
		1.1.2	The system shall utilize multifactor authentication to allow access to the system and/or sub-system, to include user to device and device-to-device. Note: If utilizing passwords see CSA 1.1.11				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to assure correct implementation of two-factor authentication.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B	Prove a valid multifactor authentication using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2 (5), IA-4, IA-8, IA-10, SC-15 CNSSI 4009 defines authentication	To Prevent a malicious devices from spoofing an already-authenticated device and gaining unauthorized access, it is important to use encryption for internal/external
		1.1.3	The system shall implement replay-resistant authentication mechanisms.				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to assure implementation of replay-resistant authentication mechanisms.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest CCs and components containing CPI are tested IAW SAE AS5553, SAE AS6171, SAE AS6081, and IDEA-STD-1010B	Prove implementation of replay-resistant authentication mechanisms using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2(8)	Replay Resistance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Replay resistance is in addition to the replay-resistant nature of authenticated protected channel protocols, since the output could be stolen prior to entry into the protected channel. Protocols that use nonces or challenges to prove the "freshness" of the transaction are resistant to replay attacks since the verifier will easily detect when old protocol messages are replayed since they will not contain the appropriate nonces or timeliness data. Examples of replay-resistant authenticators are OTP devices, cryptographic authenticators, and look-up secrets. In contrast, memorized secrets are not considered replay resistant because the authenticator output — the secret itself — is provided for each authentication. https://pages.nist.gov/800-63-3/sp800-63b.html https://www.stigviewer.com/stig/network_device_management_security_requirements_guide/2017-04-07/finding/V-55111
		1.1.4	The system shall provide a single sign-on capability.				Inspect system/subsystem and relevant documentation (e.g., interface control document, architecture, Technical Orders, SRS, SDD, drawings, configuration management plan and configuration management report) to validate the implementation of a single sign-on capability.	Utilize already created STIGs or generate system STIGs and perform Scans -HIL/SIL Simulation (loaded and normal -PIL Simulation -Failure Modes Effect Test (FMET) to include cybersecurity and resilience -100% FQT (testing) All hardware with special emphasis on lowest	Prove the implementation of single sign-on capability using the following: -Criticality Analysis -Failure Modes, Effects and Criticality Analysis (FMECA) -Attack Path Analysis	IA-2(10)	Use case

Figure A-6 Example SRD/System Specification Excel

The **System Requirements Document (SRD) and System Specifications**, identify which system level requirements are applicable to the system’s FTA. Once the system level requirements are selected, select the lower-level system requirements using the CSA worksheets. In addition to the requirements and the applicability, the Excel worksheets also contain recommended methods of verification that should be utilized for the selected requirements.

Attachment 2
Contract Data Requirements Lists Associated with SSE

Table A-15 SSE Related Contract CDRLs

Per DD Form 1423-1 Block 7, all CDRLs should specify requirement for inspection/acceptance of the data item by the Government.						
Guidebook Section SOO/SOW Reference	**CDRL**	**Name**	**Title (DD Form 1423-1, Block 2)**	**DID (DD Form 1423-1, Block 4)**	**Recommended Delivery Schedule (DD Form 1423-1, Block 12 and Block 13)**	**Recommended Remarks (DD Form 1423-1, Block 16)**
2.3.2 A	1	Program Protection Implementation Plan (PPIP)	Program Protection Implementation Plan (PPIP)	DI-ADMN-81306	60 Days after contract award Concept Plan 105 days prior to Milestone A Plan 60 days prior to PDR (or 105 days prior to Milestone B, whichever is sooner) Final Plan 60 days prior to CDR Initial AT Evaluation Plan60 days prior to PDR Final V&V Plan 60 days prior to CDR V&V Report 120 days prior to Milestone C Update annually	Follow the newest OSD PPP template
2.3.1 B 2.3.1 C	2	Specification	Program-Unique Specification Documents	DI-SDMP-81493, or DI-IPSC-81431A	Standard program delivery	
2.3.1 B 2.3.1 C	3	Specification	Interface Requirements Specification (IRS)	DI-IPSC-81434	Preliminary draft for each Configuration Item (CI) / Computer Software Configuration Item (CSCI) due 30 days prior to SFR Updates as required Final due 30 days prior to FCA for each associated CI/CSC	
2.3.1 E 2.3.3 F	4	Test Plan for all testing Laboratory, Ground, and Flight	Test Plan	DI-NDTI-80566	150 days prior to test 60 days prior to Test Readiness Review	
2.3.1 E 2.3.3 F	5	T&E Program Plan	Test and Evaluation Program Plan (TEPP)	DI-NDTI-81284	150 days prior to test 60 days prior to Test Readiness Review	
2.3.1 E 2.3.3 F	6	Software Test Plan	Software Test Plan (STP)	DI-IPSC-81438	Draft 30 days prior to PDR Final 60 days prior to Test Readiness Review	
2.3.1 E 2.3.3 F	7	Test Procedures for all testing Laboratory, Ground, and Flight	Test Procedure	DI-NDTI-80603	150 days prior to test 60 days prior to Test Readiness Review	
2.3.1 E 2.3.3 F	8	Reports for all Analysis, Inspection, Demonstration and Test	Software Test Report (STR)	DI-IPSC-81440	60 days after test 30 days prior to FCA for each associated CSCI	Configuration shall be listed on all reports and not just the under test *[e.g., the whole laboratory or aircraft with hardware part number (p/n), software version, and firmware (p/n and software version)].*
2.3.1 E 2.3.3 F	9	Reports for all Analysis, Inspection, Demonstration and Test	Test/Inspection Report	DI-NDTI-80809	Quick Look Report for 30 days after test Final 60 days after test of closure of specification 150 days prior to CDR, FCA, SVR	
2.3.2 A	10	Integrated Master Schedule (IMS)	Integrated Program Management Report (IPMR)	DI-MGMT-81861	Draft IMS due with post-award/executive kickoff meeting Second submittal due 60 days after contract award Subsequent monthly submissions start 90 days after contract award	Tailor out Sections for formats 1-5 and 7 (Sections 3.2-3.6 and Section 3.8), retaining Section 3.7 for format 6 (IMS).
2.3.2 B 2.3.1 D	11	Requirements Traceability Verification Matrix	Requirements Traceability Verification Matrix	DI-MGMT-82133	90 days prior to PDR, CDR, TRR, FCA, SVR	
2.3.1 C	12	Models, Tools and Source data for the Digital Engineering	Technical Report Study/Services (addressing Models, Tools and Source data for Digital Engineering)	DI-MISC-80508	150 days prior to SRR Updates 60 days prior to SFR/PDR/CDR/PRR/TRR/FCA/SVR/PCA and as required	Source files required to be submitted in order to execute models.

Per DD Form 1423-1 Block 7, all CDRLs should specify requirement for inspection/acceptance of the data item by the Government.

Guidebook Section SOO/SOW Reference	CDRL	Name	Title (DD Form 1423-1, Block 2)	DID (DD Form 1423-1, Block 4)	Recommended Delivery Schedule (DD Form 1423-1, Block 12 and Block 13)	Recommended Remarks (DD Form 1423-1, Block 16)
2.3.1 B **2.3.1 C** **2.3.2 C**	13	Information Security Interface Control Documents (IS-ICDs)	Interface Control Document	DI-SESS-81248	150 days prior to CDR, FCA, SVR	
2.3.1.G	14	Risk Management	Contractor Risk Management Plan	DI-MGMT-81808	60 days after contract award Updates for any changes, as required	
			Contractor Risk Management Status Report	DI-MGMT-81809	60 days prior to SRR, SFR, PDR, CDR, TRR, FCA, SVR, PRR, and PCA	
2.3.2 B2	15	Cyber Incidents	Technical Report Study/Services (addressing the Incident, Root DoDI 5200.39, and Corrective Action)	DI-MISC-80508	Draft report 24 hours after incident Final report 10 days after incident	
2.3.1 H	16	Meeting Minutes and Action Items	Conference Minutes	DI-ADMN-81250	30/60 days after meeting	
2.3.1 H	17	Agenda	Conference Agenda	DI-ADMN-81249	30 days prior to meeting	
2.3.5 D1 **2.3.5 D2** **2.3.5 D3** **2.3.5 E** **2.3.5 F** **2.3.5 G**	18	Contractor Security Plan	United States Air Force Contractor's Security Plan for Controlled Unclassified Information (CUI)	TBD	Initial at 60 days prior SRR Updated at SFR Lower level at PDR Updated at CDR	
2.3.2 B1 **2.3.3 A** **2.3.3 E** **2.3.3 G**	19	Contractor Security Plan	United States Air Force Contractor's Security Plan for Weapon Systems	TBD	Initial at 60 days prior SRR Updated at SFR Lower level at PDR Updated at CDR	For Cyber Incident reporting, follow NIST SP800-61 R2, "Computer Security Incident Handling Guide".
2.3.3 A	20	Security Assessment Report	Technical Report Study/Services (addressing the Security Assessment Report)	DI-MISC-80508	Analysis, Laboratory testing, and ground testing (with reference to test plans and procedures), traceability matrix, and architecture 120 days prior to Interim Authority To Test (IATT) Final report with all verification (Analysis, Demonstration, Inspection, and Test - with reference to test plans and procedures,) traceability matrix, and architecture 120 days prior to Authority To Operate (ATO) Update as required	
2.3.3 C	21	Failure Mode, Effects Analysis (FMEA)	Technical Report Study/Services (addressing FMEA)	RCM-FMEA DI-SESS-80980A	Functional Analysis 60 days prior to SRR/SFR Thread Analysis 60 days prior to PDR Update 60 days prior to CDR Update as required	
2.3.3 C	22	Failure Mode, Effects & Criticality Analysis (FMECA)	Failure Modes, Effects, and Criticality Analysis Report (FMECA)	DI-SESS-81495	Functional Analysis 60 days prior to SRR/SFR Thread analysis 60 days prior to PDR Update 60 days prior to CDR Update as required	
2.3.2 C **2.3.3 C** **2.3.3 D**	23	Functional Thread Analysis Report	Technical Report Study/Services (addressing Critical Components) following template in the PPP (System/Subsystem, Manufacture, P/N, etc.)	TBD	30 days after known 60 days prior to PDR 60 days prior to CDR	
2.3.1 D	24	Architect Design Document	Technical Report Study/Services (addressing architecture design)	DI-MISC-80508	Top level architecture 60 days prior to SRR/SFR Detailed architecture 60 days prior PDR Update 60 days prior to CDR Updates as required (DODAF views)	
2.3.3 E	25	Manufacturing Plan	Customized Microelectronics Devices Source Protection Plan	DI-MGMT-81763	Standard program delivery	
2.3.3 E	26	Manufacturing Plan	Counterfeit Prevention Plan	DI-MISC-81832	Standard program delivery	
2.3.3 E	27	Manufacturing Plan	Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report	DI-QCIC-80125	Standard program delivery	

Per DD Form 1423-1 Block 7, all CDRLs should specify requirement for inspection/acceptance of the data item by the Government.						
Guidebook Section SOO/SOW Reference	CDRL	Name	Title (DD Form 1423-1, Block 2)	DID (DD Form 1423-1, Block 4)	Recommended Delivery Schedule (DD Form 1423-1, Block 12 and Block 13)	Recommended Remarks (DD Form 1423-1, Block 16)
2.3.3 E	28	Manufacturing Plan	Technical Report Study/Services (addressing the Manufacturing Program Plan)	DI-MISC-80508	Standard program delivery	
2.3.3 A **2.3.3 E** **2.3.3 F**	29	Security Assessment Plan	Technical Report Study/Services (addressing the contractor Security Plan / Security Assessment Plan)	DI-MISC-80508	Initial at 60 days prior SRR Updated at SFR Lower level at PDR Updated at CDR	
2.3.3 F	30	Software Development Plan	Software Development Plan (SDP)	DI-IPSC-81427B	Preliminary draft 30 days prior to SRR Draft due 45 days after SFR DoD Anti-Tamper Technical Implementation Guide v1.0 Final due 30 days after Government approval After Government approval, contractor shall submit subsequent revisions to address contractor proposed changes	
2.3.3 F	31	Software Specifications	Software Requirements Specification (SRS)	DI-IPSC-81433	Preliminary draft for each CSCI due 30 days prior to SFR Updates as required Final due 30 days prior to FCA for each associated CSCI	
2.3.3 F	32	Software Specifications	Software Product Specification (SPS)	DI-IPSC-81441	Draft due 30 days prior to FCA for each associated CSCI Final due 30 days prior to PCA for each associated CSCI	
2.3.3 F	33	Software Test Plans and Procedures	Software Test Description (STD)	DI-IPSC-81439	30 days prior to CDR Final 60 days prior to Test Readiness Review	
2.3.3 F	34	Software Test Plans and Procedures	Technical Report Study/Services (addressing Software Development Process Description Document)	DI-MISC-80508	150 days prior to test 60 days prior to Test Readiness Review	
2.3.3 F	35	Software Test Plans and Procedures	Technical Report Study/Services (addressing Software and Programmable Logic Evaluation Report)	DI-MISC-80508	150 days prior to test 60 days prior to Test Readiness Review	
2.3.3 F	36	Software Test Plans and Procedures	System/Software Integration Laboratory (SIL) Development and Management Plan	DI-SESS-81770	Draft 30 days prior to PDR Final 60 days prior to Test Readiness Review	
2.3.3 G	37	Key and Certification Management Plan (KCMP)	Key and Certificate Management Plan (KCMP)	DI-MISC-81688	60 Days after contract award Concept Plan 105 days prior to Milestone A Plan 60 days prior to PDR (or 105 days prior to Milestone B, whichever is sooner) Final Plan 60 days prior to CDR Verification and Validation (V&V) Plan 60 days prior to PDR Final V&V Plan 60 days prior to CDR V&V Report 120 days prior to Milestone C Updated annually	
2.3.3 H	38	TEMPEST	TEMPEST Control Plan	DI-MGMT-81026	150 days prior to test Final 30 days after test completion	
2.3.3 H	39	TEMPEST	TEMPEST Test Plan	DI-EMCS-81683	150 days prior to test Final 30 days after test completion	
2.3.3 H	40	TEMPEST	TEMPEST Test Evaluation Report	DI-EMCS-81684	150 days prior to test Final 30 days after test completion	
2.3.3 B	41	Data Accession List	Data Accession List (DAL)	DI-MGMT-81453	Immediate access to DAL items which are electronically available First submittal of the DAL index shall be submitted 30 days after contract award and quarterly thereafter For paper copies, the contractor shall submit its internal data within 10 working days, but no more than 20 days after receipt of the Procuring Contract Officer Letter (PCOL) from the procuring agency For paper copies the contractor shall submit subcontractor data within 15 working days, but not later than 25 days after receipt of PCOL from procuring agency	

Per DD Form 1423-1 Block 7, all CDRLs should specify requirement for inspection/acceptance of the data item by the Government.

Guidebook Section SOO/SOW Reference	CDRL	Name	Title (DD Form 1423-1, Block 2)	DID (DD Form 1423-1, Block 4)	Recommended Delivery Schedule (DD Form 1423-1, Block 12 and Block 13)	Recommended Remarks (DD Form 1423-1, Block 16)
2.3.4 A	42	AT Plan	Technical Report Study/Services (addressing the AT Plan (PPP Appendix D))	DI-MISC-80508	AT Concept Plan 105 days prior to Milestone A Initial AT Plan 60 days prior to PDR (or 105 days prior to Milestone B, whichever is sooner) Final AT Plan 60 days prior to CDR Initial AT Evaluation Plan 60 days prior to PDR Final AT Evaluation Plan 60 days prior to CDR	**NOTE:** Distribution should include the Government program office and the USAF Anti-Tamper Evaluation Team (ATET) to facilitate timely review and comments.
2.3.4 A	43	AT Verification Report	Technical Report Study/Services (addressing the Anti-Tamper (AT) Verification Report)	DI-MISC-80508	Initial report with analysis and laboratory test plan procedures and reports 60 days prior to CDR V&V Report 120 days prior to SVR or Milestone C	
2.3.3 F	44	Information Security (INFOSEC) Boundary Configuration Management Plan	Information Security (INFOSEC) Boundary Configuration Management Plan	DI-SESS-81343	Standard program delivery	
2.3.5 A	45	Operations Security (OPSEC) Plan	Operations Security (OPSEC) Plan	DI-MGMT-80934	Standard program delivery	
2.3.1 B	46	DoD Modeling and Simulation (M&S) Accreditation Plan	Department Of Defense (DoD) Modeling and Simulation (M&S) Accreditation Plan	DI-MSSM-81750	60 days prior to PDR Update as required	
2.3.1 B	47	DoD Modeling and Simulation (M&S) Accreditation Report	Department Of Defense (DoD) Modeling and Simulation (M&S) Accreditation Report	DI-MSSM-81753	60 days prior to CDR Update as required	
2.3.1 E	48	DoD M&S Verification and Validation (V&V) Plan	Department Of Defense (DoD) Modeling and Simulation (M&S) Verification and Validation (V&V) Plan	DI-MSSM-81751	60 days prior to PDR Update as required	
2.3.1 E	49	DoD M&S Verification and Validation (V&V) Report	Department Of Defense (DoD) Modeling and Simulation (M&S) Verification and Validation (V&V) Report	DI-MSSM-81752	60 days prior to CDR Update as required	
2.3.2 C	50	Attack Path Analysis Report	Software Attack Surface Analysis Report; Additional option is: Technical Report Study/Services (addressing Attack Path Analysis)	DI-IPSC-82250 DI-MISC-80508	Initial analysis 60 days prior to PDR Update 60 days prior to CDR Final 60 days prior to FCA / SVR Update as required	
2.3.3 E	51	Acceptance Test Plan	Technical Report Study/Services (addressing Acceptance Test Plan)	DI-MISC-80508	Initial analysis 60 days prior to PDR Update 60 days prior to CDR Final 60 days prior to FCA / SVR Update as required	
2.3.3 E	52	Acceptance Test Procedure	Technical Report Study/Services (addressing Acceptance Test Procedures)	DI-MISC-80508	Initial analysis 60 days prior to PDR Update 60 days prior to CDR Final 60 days prior to FCA / SVR Update as required	
2.3.3 E	53	Acceptance Test Report	Acceptance Test Report (ATR)	DI-QCIC-81891	30 days after test completion	
2.3.3 A	54	Plan of Action and Milestones	Technical Report Study/Services (addressing Plan of Action and Milestones)	DI-MISC-80508	Initial analysis 60 days prior to PDR Update 60 days prior to CDR Final 60 days prior to FCA / SVR Update as required	

Per DD Form 1423-1 Block 7, all CDRLs should specify requirement for inspection/acceptance of the data item by the Government.						
Guidebook Section SOO/SOW Reference	**CDRL**	**Name**	**Title (DD Form 1423-1, Block 2)**	**DID (DD Form 1423-1, Block 4)**	**Recommended Delivery Schedule (DD Form 1423-1, Block 12 and Block 13)**	**Recommended Remarks (DD Form 1423-1, Block 16)**
2.3.3 A **2.3.3 F**	55	Configuration Management Plan	Technical Report Study/Services (addressing overall System Configuration)	DI-CMAN-80858B	60 days prior to PDR Update as required	
2.3.3 A **2.3.3 F**	56	Configuration Management Report	Technical Report Study/Services (addressing overall System Configuration)	DI-SESS-81022D	Initial analysis 60 days prior to PDR Update 60 days prior to CDR Final 60 days prior to FCA / SVR Update as required	
2.3.3 F	57	Software Development Description	Software Design Description (SDD)	DI-IPSC-81435	Preliminary draft due 30 days prior to PDR for each CSCI Updates as required Final due 30 days prior to FCA for each associated CSCI	
2.3.1 F	58	SSE Requirements Implementation Assessment	Technical Report Study/Services (addressing SSE Requirements Implementation Assessment)	DI-MISC-80508	90 days prior to SRR, SFR, PDR, CDR, TRR, FCA, SVR, PRR, and PCA	
2.3.1.G	59	System Safety Plan	System Safety Plan	DI-SAFT-81626	60 days prior to CDR Updates, as required	
2.3.1.G	60	Hazard Assessment	System Safety Hazard Analysis Report	DI-SAFT-80101	60 days prior to CDR Update, if required, 150 days prior to first aircraft delivery	
2.3.1 A	61	Systems Engineering Management Plan (SEMP)	Systems Engineering Management Plan (SEMP)	DI-SESS-81785A	"As per the Contract Delivery Table listed on the DD Form 1423	
2.3.2 B3	62	Forensic Readiness Plan	Technical Report Study/Services (addressing the Forensic readiness plan)	DI-MISC-80508	Draft report 20 days after contract award Final report 15 days after Government review of draft	Follow NIST SP800-171 R2, “Protecting CUI in Non-Federal Systems and Organizations”, and NIST SP800-53 “Security and Privacy Controls for Federal Information Systems and Organizations
2.3.2 B3	63	Forensic Analysis & Corrective Action	Technical Report Study/Services (addressing the Forensic readiness plan, Root Cause analysis and Corrective Action)	DI-MISC-80508	Draft report 10 days after incident Final report 15 days after Government review of draft	

Attachment 3
SOO/SOW SSE Requirements Trace

Table A-16 SOO/SOW SSE Requirements Traceability Table

2.3.1 Overall Systems Security Engineering	NIST SP800-53r5 Control Family References	CSEIG "Highly Applicable" Mapping
A	SA	CSA 08
B	SA	CSA 08
C	SA	CSA 08
D	CA, SA, SC	CSA 05, CSA 06, CSA 08
E	CA, RA	CSA 04, CSA 06, CSA 07
F	CA, RA, SA	CSA 04, CSA 06, CSA 07, CSA 10
G	CA, RA, SA	CSA 04, CSA 06, CSA 07, CSA 10
H	SA	CSA 08
2.3.2: Program Protection	**NIST SP800-53r5 Control Family References**	**CSEIG "Highly Applicable" Mapping**
A	AC, CA, CP, IR, SA, SC, SI	CSA 01, CSA 06, CSA 07, CSA 08, CSA 09, CSA 10
B	SA, RA, SC, SI	CSA 06, CSA 07, CSA 08, CSA 09
C	CA, SA, SC	CSA 03, CSA 05, CSA 06, CSA 08
2.3.3: Cybersecurity and Trusted Systems and Networks	**NIST SP800-53r5 Control Family References**	**CSEIG "Highly Applicable" Mapping**
A	AC, CA, CM, IA, MA, MP, PL, PS, RA	CSA 06, CSA 07, CSA 10
B	SA, RA	CSA 06, CSA 08
C	SA, SC, CM, RA	CSA 06, CSA 07, CSA 10
D	AC, PL, SA, SC, RA	CSA-01, CSA 06, CSA 08
E	AC, MA, SA, RA	CSA 01, CSA 06, CSA 08, CSA-10
F	AC, AU, CA, CM, CP, IA, IR, PL, RA, SA, SC	CSA-01, CSA 06, CSA 08
G	AC, CA, CM, IA, PL, SA, SC	CSA-01, CSA 06, CSA 08
H	PE, PL	[None]
2.3.4: Critical Program Information (CPI) / Anti-Tamper (AT)	**NIST SP800-53r5 Control Family References**	**CSEIG "Highly Applicable" Mapping**
A	AC, PE, SA	CSA 01, CSA 08

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

APPENDIX B

CRITICAL PROGRAM INFORMATION (CPI) AND CRITICAL COMPONENTS (CC)

Version 4.0

26 July 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Secretary of the Air Force, Public Affairs (SAF/PA) Case #: 2021-0424. Requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

Table of Contents

Table of Tables

Table of Figures

Executive Summary

During program protection planning, a set of activities is performed to manage the execution of program protection. Two early and foundational processes include the Critical Program Information (CPI) Identification Process and the Critical Component (CC) Identification Process. The CPI and CC Identification Processes have been completely separate and distinct processes conducted by programs.

Department of the Air Force (DAF) programs recognized the need to reduce redundancy and increase efficiency of the separate CPI/CC Identification Processes. This guide consolidates the CPI and CC Identification Processes and identifies a fully integrated process. Programs conducting a combined CPI/CC Identification Process should realize significant improvement in the efficiency and effectiveness of these processes. Programs conducting the CPI Identification Process only or the CC Identification Process only will also be able to use this guide.

FOREWARD

“USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components (CC)” introduces the processes involved to accurately identify, secure an independent review and approval of a program’s CPI/CC to the reader.

Record of Changes

Version	Effective	Summary
4.0	26 July 2021	Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	Addition of Space Systems into SSE requirements assessment process.
3.0.1	29 January 2021	No changes to content, just updated revision numbers to correspond with body of the main document.

1.0. Introduction

During program protection planning, a set of activities is performed to manage the execution of program protection. The CPI Identification Process and the CC Identification Process are important processes in program protection planning. Until recently, the CPI and CC identification processes have been separate processes conducted independently by programs. Several steps are common between the two analyses, requiring programs to repeat some steps during the conduct of the separate processes. These overlapping steps have resulted in inefficient processes being performed by programs. USAF programs recognized the need for a combined CPI/CC Identification Process to reduce redundancy and increase efficiency. This guide incorporates the details of the CPI and CC Identification processes and identifies common elements to both. The two processes have been integrated into a “combined process” to allow for improved efficiency and effectiveness.

1.1. Background

CPI and CC identification are important processes that the Department of Defense (DoD) requires programs to apply to their National Security Systems (NSS). These processes are essential to the successful development of a Program Protection Plan (PPP). The following DoD Instructions (DoDIs) establish the requirement to identify and protect CPI and CCs:

- DoDI 5200.39, CPI Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), Incorporating Change 1 [1]
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), Incorporating Change 2 [2]

1.2. Purpose

The purpose of this process guide is to provide recommended guidance that enables programs to accurately identify and obtain independent review and approval of CPI/CC. The activities and descriptive tasks identified in this document are provided only as guidance and should not be interpreted as the only approach for CPI/CC identification that suffices for all aspects of every program. Each program is encouraged to apply the provided guidance in a manner that complements and/or extends current Systems Security Engineering (SSE) approaches regarding the identification and protection of CPI and CCs when developing, modifying or upgrading their system(s).

2.0. Process Definition

“Program Protection” is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle” [3]. One of the most important steps in the program protection planning process is the identification of CPI and CCs. Knowing what is important to protect allows a program to develop an effective and efficient strategy to follow throughout (or across) the life cycle.

CPI/CC identification consists of broad SSE activities that may extend to many stakeholders, such as the Program Lead/Chief Engineers (CEs), Program Subject Matter Experts (SMEs), development contractors, and the broader program Systems Engineering (SE) community. This process guide explains the identification of CPI/CC[28] for the system-of-interest and the enabling systems with National Security importance.

CPI/CC is to be identified early in the Integrated Life Cycle (ILC), and continuously managed such that informed decisions regarding the engineering, operation, and sustainment of systems consider the CPI/CC that resides with the system or is represented by system capabilities. Proper identification, vetting, and tracking of CPI/CC serve as means to more effectively manage the life cycle costs driven by systems security. Additionally, the timing, scope, and rigor, in application of the CPI/CC identification analysis, ensure that the optimal effort is expended to determine what CPI/CC exists and to protect it in a cost-effective and risk-tolerant manner.

The identified CPI/CC shall be approved by the Milestone Decision Authority (MDA)[29]. The approved CPI/CC is maintained under configuration management by the program, documented in the PPP, and reviewed at every Systems Engineering Technical Review (SETR) and Milestone Decision. The program's Configuration Control Board shall review security/Cyber Resiliency impacts to CPI/CC when considering change proposals to the system. Any change in the status of the CPI/CC (e.g., new CPI/CC added, CPI/CC removed, technology used in CPI/CC aged, change in threats to CPI/CC) requires this process be revisited. Any change in the missions, system, how the system is used to support the missions, or in the development and sustainment of the system also requires this process be revisited. This ensures that U.S. NSSs continue to remain uncompromised and maintain their technological advantage and security posture.

3.0. Integrated CPI and CC Identification Process Flow

The integrated CPI and CC Identification Process Flow (**Figure B-1**) provides an overview depiction of the integrated CPI/CC Identification Process. The overall flow is separated into three columns: Engineering Analysis Results, Technical Analysis Flow, and Government Stakeholder Coordination:

- Engineering Analysis Results: The left column identifies where the results of evidence-based analysis and engineering trades are captured.

[28] The identification of Critical Program Information (CPI)/Critical Component (CC) is conducted as part of systems security engineering (SSE) requirements elicitation and requirements analysis activities. Consult Institute of Electrical and Electronics Engineers (IEEE) Standard 15288 “Systems and Software Engineering – Systems Lifecycle Processes” for discussion of requirements elicitation and analysis oriented to all system requirements, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 “Systems Security Engineering” for discussion of requirements elicitation and analysis oriented to security requirements. For definitions of “system-of-interest” and “enabling system,” see International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) International Standard 15288:2015 [4] or Appendix B, Table B-5.

[29] The Program Executive Officer (PEO) and MDA may have different roles and responsibilities depending upon the ACAT level of the program. In some cases, the Program Executive Officer may be the MDA.

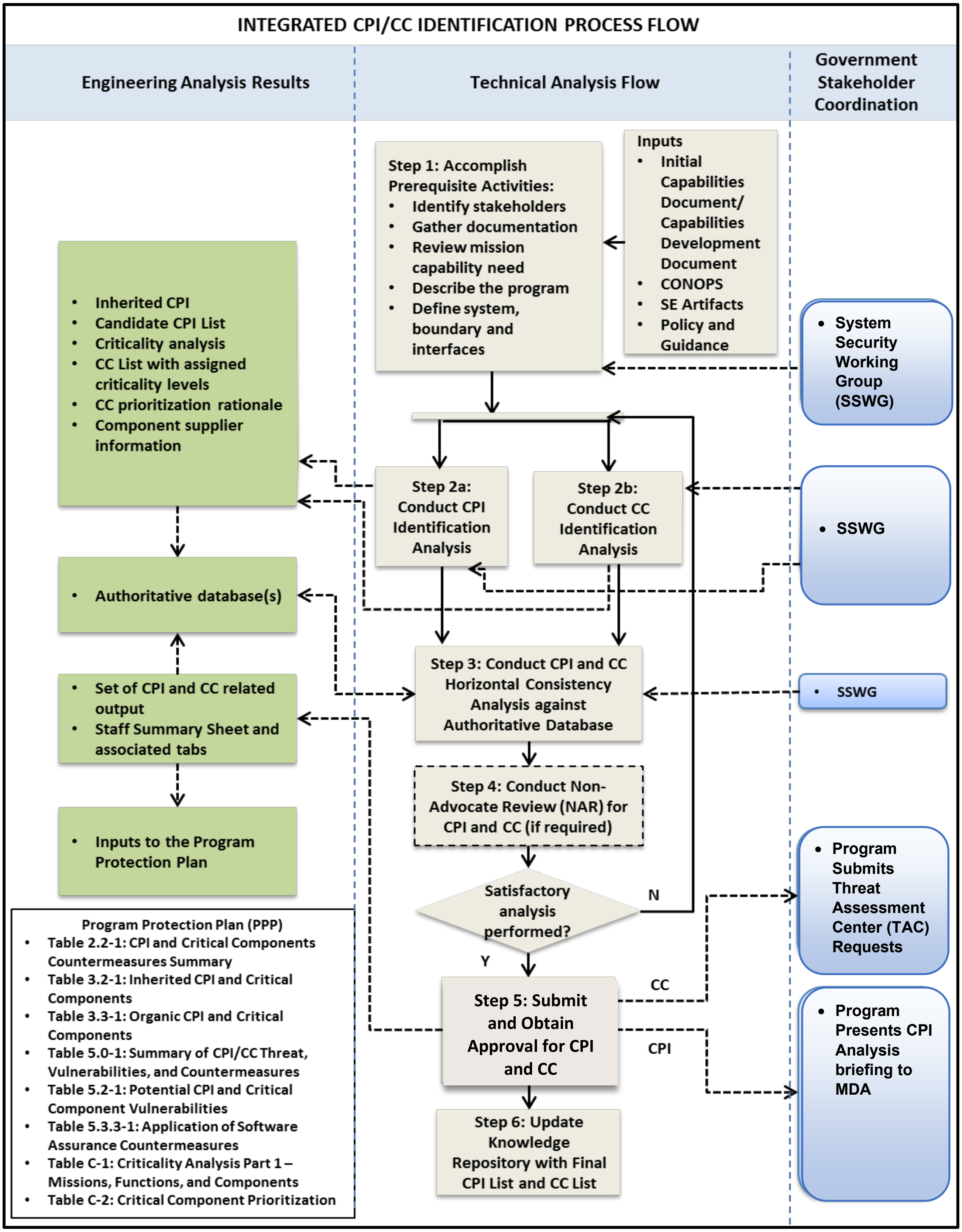
NOTE: The list of Tables in the "Program Protection Plan (PPP)" box is from the Program Protection Plan Outline & Guidance, Version 1.0 [5].

- Technical Analysis Flow: The middle column outlines the technical analyses required to identify the CPI and CC items, to assign criticality levels to CCs, and to produce the evidence-based analysis results that are captured in the artifacts cited in the left column. Further, the column identifies the documents, policies, and instructions that programs should consider as inputs to the activities identified. The identified documents, policies, and instructions do not constitute an exhaustive list of sources that inform the analyses conducted. The program needs to determine and leverage all relevant sources of information to properly conduct the evidence-based analyses.

- Government Stakeholder Coordination: The right column identifies when, in the process, programs should coordinate with their stakeholders. The importance of coordination is to ensure that programs provide the opportunity to inform their stakeholders, early on in their process, of how they are conducting the CPI and CC identification processes and receive feedback throughout the analysis. Programs should ensure that all relevant stakeholders are involved in the process of identifying CPI and CCs, as required by, and as necessary to support, the program-defined agreements, milestones, and related needs and constraints. Based on the complexity of the analysis and the number of agencies/organizations involved in a program, additional coordination steps may be required

Significant information associated with a specific program/ space and weapon system/NSS is generated during the CPI and CC Identification Process. This information includes the completed CPI and CC Tables with criticality levels and other mission critical information. Much of this data becomes classified and should be handled with the applicable commensurate protections.

Figure B-1 Integrated CPI and CC Identification Process Flow

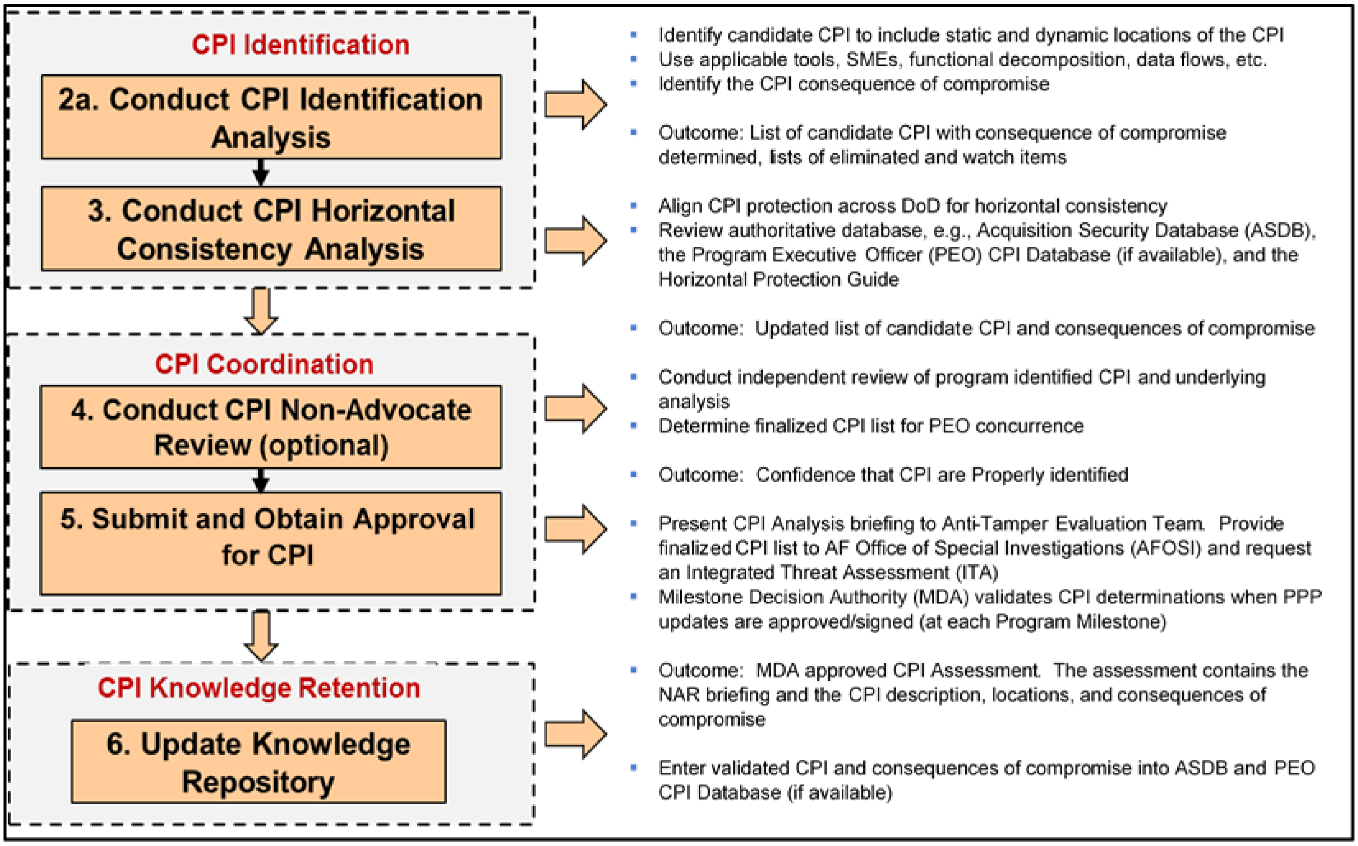

INTEGRATED CPI/CC IDENTIFICATION PROCESS FLOW
Engineering Analysis Results
Technical Analysis Flow
Government Stakeholder Coordination
Step 1: Accomplish Prerequisite Activities:
• Identify stakeholders
• Gather documentation
• Review mission capability need
• Describe the program
• Define system, boundary and interfaces
Inputs
• Initial Capabilities Document/ Capabilities Development Document
• CONOPS
• SE Artifacts
• Policy and Guidance
• System Security Working Group (SSWG)
• Inherited CPI
• Candidate CPI List
• Criticality analysis
• CC List with assigned criticality levels
• CC prioritization rationale
• Component supplier information
Step 2a: Conduct CPI Identification Analysis
Step 2b: Conduct CC Identification Analysis
• SSWG
• Authoritative database(s)
Step 3: Conduct CPI and CC Horizontal Consistency Analysis against Authoritative Database
• SSWG
• Set of CPI and CC related output
• Staff Summary Sheet and associated tabs
Step 4: Conduct Non-Advocate Review (NAR) for CPI and CC (if required)
• Inputs to the Program Protection Plan
Satisfactory analysis performed?
N
Y
• Program Submits Threat Assessment Center (TAC) Requests
Step 5: Submit and Obtain Approval for CPI and CC
CC
CPI
• Program Presents CPI Analysis briefing to MDA
Step 6: Update Knowledge Repository with Final CPI List and CC List
Program Protection Plan (PPP)
• Table 2.2-1: CPI and Critical Components Countermeasures Summary
• Table 3.2-1: Inherited CPI and Critical Components
• Table 3.3-1: Organic CPI and Critical Components
• Table 5.0-1: Summary of CPI/CC Threat, Vulnerabilities, and Countermeasures
• Table 5.2-1: Potential CPI and Critical Component Vulnerabilities
• Table 5.3.3-1: Application of Software Assurance Countermeasures
• Table C-1: Criticality Analysis Part 1 – Missions, Functions, and Components
• Table C-2: Critical Component Prioritization

4.0. Individual CPI and CC Identification Processes

Programs conducting the CPI Identification Process only or the CC Identification Process only can also use this guide. Whether performing only one process (CPI Identification or CC Identification) or the integrated CPI/CC Identification Process, the prerequisite activities described in Step 1 (Section **Error! Reference source not found.**) are conducted first. Programs executing a single process will then conduct the relevant guidance within each step, as appropriate.

4.1. Individual CPI Identification Process

For programs executing only the CPI Identification Process, refer to Figure B-2. This figure can be used to maintain focus on the CPI Identification Process being executed by your program. Each rectangle in this figure corresponds with the associated step number (i.e., steps 2a, 3, 4, 5, and 6) in Figure B-1 and discussed later in this guide. The relevant content in the associated Sections provide the guidance needed to execute each step.

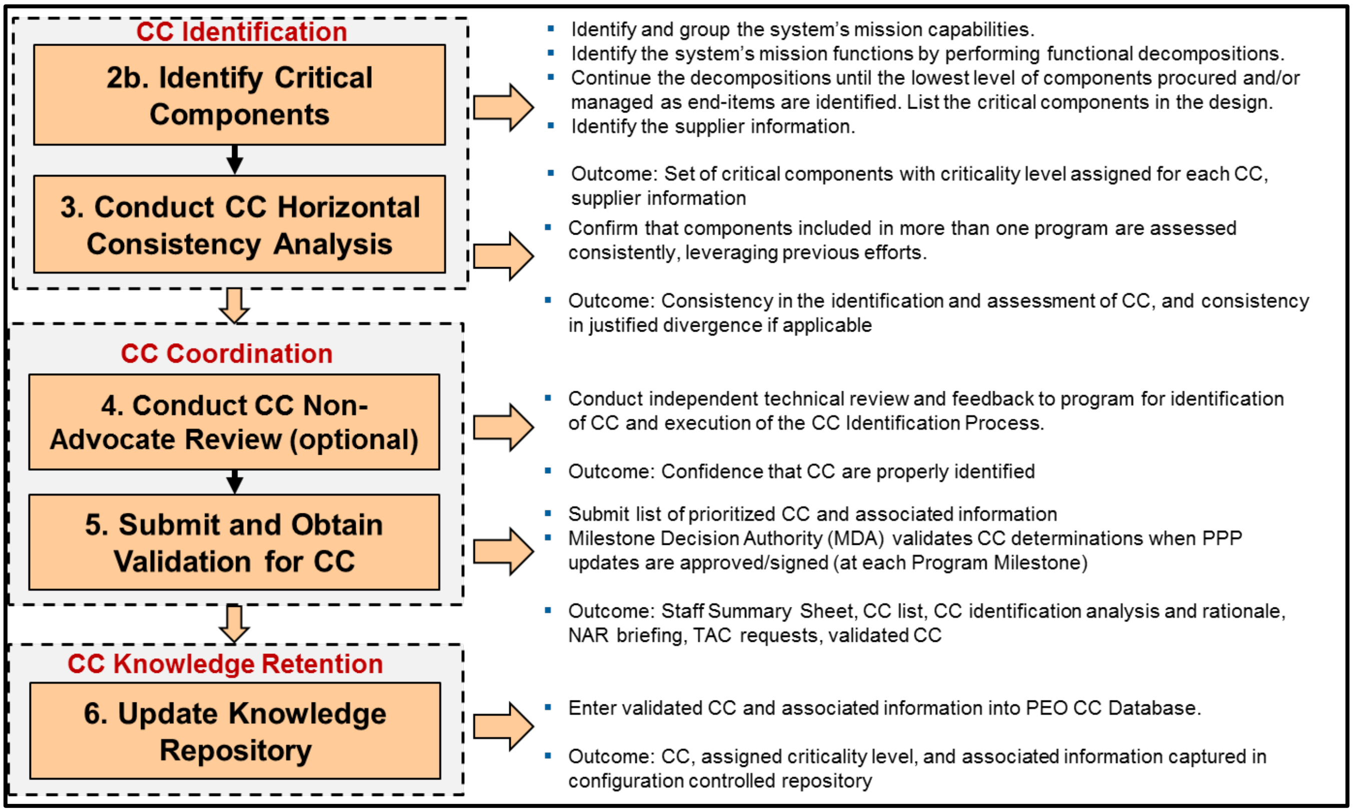

CPI Identification
2a. Conduct CPI Identification Analysis
3. Conduct CPI Horizontal Consistency Analysis
CPI Coordination
4. Conduct CPI Non-Advocate Review (optional)
5. Submit and Obtain Approval for CPI
CPI Knowledge Retention
6. Update Knowledge Repository

- Identify candidate CPI to include static and dynamic locations of the CPI
- Use applicable tools, SMEs, functional decomposition, data flows, etc.
- Identify the CPI consequence of compromise
- Outcome: List of candidate CPI with consequence of compromise determined, lists of eliminated and watch items
- Align CPI protection across DoD for horizontal consistency
- Review authoritative database, e.g., Acquisition Security Database (ASDB), the Program Executive Officer (PEO) CPI Database (if available), and the Horizontal Protection Guide
- Outcome: Updated list of candidate CPI and consequences of compromise
- Conduct independent review of program identified CPI and underlying analysis
- Determine finalized CPI list for PEO concurrence
- Outcome: Confidence that CPI are Properly identified
- Present CPI Analysis briefing to Anti-Tamper Evaluation Team. Provide finalized CPI list to AF Office of Special Investigations (AFOSI) and request an Integrated Threat Assessment (ITA)
- Milestone Decision Authority (MDA) validates CPI determinations when PPP updates are approved/signed (at each Program Milestone)
- Outcome: MDA approved CPI Assessment. The assessment contains the NAR briefing and the CPI description, locations, and consequences of compromise
- Enter validated CPI and consequences of compromise into ASDB and PEO CPI Database (if available)

Figure B-2 CPI Identification Process

4.2. Individual CC Identification Process

For programs executing only the CC Identification Process, refer to Figure B-3. This figure can be used to maintain focus on the CC Identification Process being executed by your program. Each rectangle in this figure corresponds with the associated step number (i.e., steps 2b, 3, 4, 5, and 6) discussed later in this guide. The relevant content in the associated Sections provide the guidance needed to execute each step.



CC Identification

2b. Identify Critical Components

- Identify and group the system's mission capabilities.
- Identify the system's mission functions by performing functional decompositions.
- Continue the decompositions until the lowest level of components procured and/or managed as end-items are identified. List the critical components in the design.
- Identify the supplier information.

- Outcome: Set of critical components with criticality level assigned for each CC, supplier information

3. Conduct CC Horizontal Consistency Analysis

- Confirm that components included in more than one program are assessed consistently, leveraging previous efforts.

- Outcome: Consistency in the identification and assessment of CC, and consistency in justified divergence if applicable

CC Coordination

4. Conduct CC Non-Advocate Review (optional)

- Conduct independent technical review and feedback to program for identification of CC and execution of the CC Identification Process.

- Outcome: Confidence that CC are properly identified

5. Submit and Obtain Validation for CC

- Submit list of prioritized CC and associated information
- Milestone Decision Authority (MDA) validates CC determinations when PPP updates are approved/signed (at each Program Milestone)

- Outcome: Staff Summary Sheet, CC list, CC identification analysis and rationale, NAR briefing, TAC requests, validated CC

CC Knowledge Retention

6. Update Knowledge Repository

- Enter validated CC and associated information into PEO CC Database.

- Outcome: CC, assigned criticality level, and associated information captured in configuration controlled repository

Figure B-3 CC Identification Process

5.0. Step 1: Accomplish CPI/CC Identification of Prerequisites

The following subsections describe the five prerequisite activities that lead to more efficient execution of the CPI and CC identification analyses: (1) identify the stakeholders, (2) gather documentation, (3) review the capability need and objectives, (4) describe the program, and (5) establish a technical/engineering foundation.

5.1. Identify the Stakeholders

All stakeholders that may impact, be impacted by, or contribute their area of expertise, for the system-of-interest (and its enabling systems) throughout its life cycle should be identified. Stakeholders involved with the program include the following organizations and individuals, at a minimum; additional stakeholders may also pertain to your program:

PEOs.

- Directorate or division-level management.
- Program Managers (PMs).
- Chief Engineer (CE).
- Lead Engineers (LEs).
- Systems Security Engineers.

SMEs.

- DoD components, including agencies involved with funding, policy, contracting, acquisition, testing, maintenance, and logistics, Intelligence, counterintelligence (CI), Information Protection (IP), Foreign Disclosure Officer (FDO), Office of Special Investigation (OSI) and security.

MDA.

- Development contractors.
- Sustainment contractors.
- Users of the system.

Each stakeholder's role(s), their concerns, and the information they have, should be identified. Key stakeholders, those with decision-making authority concerning the system, should be identified from the stakeholder list.

5.2. Gather Documentation

Following stakeholder identification, the pertinent documents should be gathered. Table B-1 identifies the types of documents that should be obtained from existing engineering and other data. Subsequent activities will utilize the gathered documentation. Some documents that are not available early on, may become available later in the process.

Table B-1 Information and Documentation Sources

Type of Information Needed	Description	Relevant Artifacts
Program Description	Program overview, phase	• Acquisition Strategy Panel (ASP); Overview and Summary Information (AV-1); Operational Requirements Document
Program Schedule	Schedules, milestones	• Work Breakdown Structure (WBS); Integrated Master Schedule
System Architecture/Design	Picture/diagram of system	• High Level Operational Concept Graphic (Operational Viewpoint [OV-1]) • Information Security Capability Development Document (IS-CDD) • Concept of Operations (CONOPS) • System Requirements Document (SRD) • Key Performance Parameters (KPPs) • Key System Attributes (KSAs) • Systems Functionality Description (Systems Viewpoint [SV-4]) • Operational Activity to Systems Function Traceability Matrix (SV-5a) • Operational Activity to Systems Traceability Matrix (SV-5b) • Operational Resource Flow Matrix (OV-3) • Capability to Operational Activities Mapping (CV-6) • Use Cases • System Architecture • System Specification/Subsystem Specification • Configuration Item (CI) and sub-CI specifications • Information Security Initial Capabilities Document (IS-ICD) • System Performance Specification

Type of Information Needed	Description	Relevant Artifacts
Functional Decomposition		- Systems Functionality Description (SV-4) - Operational Activity Decomposition Tree (OV-5a) - Operational Activity Model (OV-5b) - Operational Activity to Systems Function Traceability Matrix (SV-5a) - Operational Activity to Systems Traceability Matrix (SV-5b)
Data Flows	Security	- Systems Interface Description (SV-1) - Systems Resource Flow Description (SV-2) - Operational Resource Flow Description (OV-2) - Operational Activity Model (OV-5b); Interface Design Document (IDD) - Interface Control Document - Data flow diagrams
Design Information		- Preliminary Design Review (PDR) materials - Critical Design Review (CDR) materials - Software Design Document (SDD)
Other artifacts	As available	- Acquisition Plan (AP) - Acquisition Strategy - Analysis of Alternatives (AoA) - Bill of Materials (BOM) - Contractor Intellectual Property (IP) assertions - Cybersecurity Strategy - Engineering Development Documents - DoDM S-5230.28 - Failure Modes and Effects Analysis (FMEA) - Foreign Military Sales (FMS) Letter of Agreement (LOA) - FMS Letter of Requirement (LOR) - CPI Horizontal Protection Guidance (HPG) - Information Support Plan (ISP)

Type of Information Needed	Description	Relevant Artifacts
		• Key Management Plan (KMP) • Lifecycle Sustainment Plan (LCSP) • Line Replaceable Units (LRU) list • Performance-Based Agreements (PBAs) • Product Support Strategy (PSS) • Provisos • Related technology DMs from similar systems • Requirements Traceability Verification Matrix • Program Protection Plan • Security Classification Guide (SCG) • Security Letters from inherited CPI • Software Development Plan (SDP) • System Sustainment Documents • System/Segment Design Document (SSDD) • Systems Engineering Plan (SEP) • Systems Technology and Skills Forecast (SV-9) • Technical Orders (TOs) • Technical Studies/Technical Analyses • Technology Readiness Assessment (TRA)[30] • Test and Evaluation Master Plan (TEMP) • Tri-Service Committee (TSC) or Executive Committee of the National Security Council (EXCOM) Decision Memorandums (DMs) from the program • Use Cases • Validated On-line Life-cycle Threat (VOLT) Report

[30] GAO-20-48G TRA Guide, “Technology Readiness Assessment Guide”

5.3. Review Capability Need and Objectives

Next, the mission capability need and objectives, including any available requirements, should be described. An understanding of the system mission provides context and important information concerning the capabilities that the system is to deliver. The program responsible for delivering the system will be aware of the scope of the system. This information provides a basic understanding of the User needs to be met by the system-of-interest and the expected outcome of the acquisition. This understanding may be obtained by perusing the IS-ICD, CONOPS, and SRD.

The CPI/CC analysis should be accomplished within the program's assumptions and constraints. Assumptions and constraints should not be arbitrary, but should be founded upon expert judgments rendered by experienced program and technical personnel. A list of assumptions and constraints concerning the program, if not already available, should be generated and agreed upon. Such a list will help ensure that the team conducting the analysis will be operating from the same foundation upon which the analysis will be built.

5.4. Describe the Program

The program that has been established to achieve the expected acquisition outcome should be described. This information includes the following aspects, with respect to the system-of-interest:

- Context for the system-of-interest (i.e., how it fits into a broader "system").
- Acquisition agencies involved in the program and how the program is linked to other ongoing efforts.
- Milestones.
- Resources (e.g., funds, equipment, facilities, and training) assigned to the program.
- Environments in which the system-of-interest will operate.
- Enabling systems, such as development systems, test systems, simulation systems, training systems, and maintenance systems, and their locations.
- Locations of design, development, testing, manufacturing, and sustainment facilities.
- Other systems that interact with the system-of-interest in its operational environment, but that are external to the system boundary.
- Foreign interactions (e.g., Foreign Military Sales [FMS], Direct Commercial Sales [DCS], Defense Exportability Features [DEF]).
- Concept of Operations (CONOPS), especially CONOPS that are different from the design criteria for the inherited CPI
- Export capabilities and strategy including Defense Exportability Features
- Describe the entire system, and describe the subset (if any) for which the CPI analysis is being performed. Highlight any conceptually defined aspects of the system that will require CPI analysis at a later date. Include the operationally deployed system, as well as, all deliverables (test equipment, Special Test equipment (STE), simulations, trainers, etc.)

- Identify subsystems, assemblies, or components procured or co-developed / co-produced from foreign sources, including HW/SW/FW
- Identify all subsystems, assemblies, or components that are re-used from other programs
- Identify any CPI these systems introduce, as well as, the program(s) from which it is inherited
- Identify whether Government-to-Government coordination may be required for re-use
- Identify any CPI which may enter the system dynamically from outside the system, but not necessarily stored statically within the system
- Identify the system block diagram and external interfaces to the extent available for the acquisition phase

5.5. Establish Technical/Engineering Foundation

The basis for the combined CPI/CC Identification Process is the establishment of a defined boundary for what is included in the system-of-interest, what systems interface to the system-of-interest, and what systems are external to the system boundary. If the system-of-interest fits within a larger system, then that context should be described. It is also important to define the enabling systems along with their boundaries and interfaces. Where a legacy capability exists, it is critical to first understand the capability baseline. A clear description of the upgrade then needs to be presented to support the definition of the system boundary.

Once the system boundary has been identified, the focus can shift to the system-of-interest to identify the system elements/components that it contains. For each element that comprises the system-of-interest, its blocks should be detailed, focusing on the uniqueness of the blocks, how they interface to one another, and how data is passed between them. Convergence should continue until the system is sufficiently detailed, allowing an assessment of each distinct function.

5.5.1. Define the System Including the System-of-Interest and its Enabling System

Summary: The identification and definition for the system-of-interest , as well as, the collection of enabling systems that provide service for the system-of-interest sets the foundation for the identification of CPI and CC.[31]

Potential Inputs:

- CONOPS.
- IS-ICD/IS-CDD.
- ISP.
- KPPs.
- Use Cases.

[31] Some enabling systems may not be known at initial milestones or Systems Engineering Technical Reviews.

- High Level Operational Concept Graphic (OV-1).
- Operational Activity Decomposition Tree (OV-5a).
- Operational Activity Model (OV-5b).
- TOs, when available.

Outcome:

- A system description that identifies the system, its program, what the system-of-interest is intended to accomplish, and what enabling systems are also going to be implemented or used for training and sustainment activities.

Guidance:

Task 1.1: Identify the system mission and describe the program that is assigned to deliver the capability. The program description should include the location(s) where the system is being designed/developed and deployed.

Task 1.2: Define the system-of-interest that is the focus of the engineering effort.

Task 1.3: Define the enabling systems for the system-of-interest (including locations).

5.5.2. Define Boundary and Interfaces for System-of-Interest and its Enabling System

Summary: An understanding of the boundary and interfaces for the system-of-interest and the enabling systems will identify the scope for the engineering focus. Engineering efforts depend on a clear demarcation of the boundary and well-defined system interfaces.

Potential Inputs:

- Data flow diagrams.
- Systems Interface Description (SV-1).
- Interface Control Document.
- IDD.
- TOs, when available.

Outcomes:

- Delineation of the boundary and interfaces for the system-of-interest.
- Delineation of the boundary and interfaces for the enabling systems.
- System diagrams depicting the boundary and interfaces for the system-of-interest and each enabling system.

Guidance:

Task 2.1: Define the boundary and interfaces for the system-of-interest. The system boundary for the system-of-interest will also include its system elements, but should not include portions of the larger system that are not included in the program's focus. The definition of interfaces includes those with other systems in the operational environment, as well as, the enabling systems. Interfaces with any industrial control systems should be included in the analysis.

Task 2.2: Define the boundary and interfaces for each enabling system.

5.5.3. Identify the System Elements that Compose the System

Summary: The subsystems/major elements that the system-of-interest and enabling systems contain should be identified. For each element that comprise the system-of-interest and enabling systems, their blocks should be detailed, focusing on the uniqueness of the blocks, how they interface to one another, and how data is passed between them.

Potential Inputs:

- Data flow diagrams.
- Systems Interface Description (SV-1).
- Interface Control Document.
- IDD.
- TOs, when available.

Outcome:

- System diagrams depicting the subsystems and major elements for the system-of-interest and each enabling
system.

Guidance:

Task 3.1: Define the subsystems and major elements in the system-of-interest.

Task 3.2: Identify the interfaces and data flows between the subsystems and major elements associated with the system-of-interest.

Task 3.3: Define the subsystems and major elements in each enabling system.

Task 3.4: Identify the interfaces and data flows between the subsystems and major elements within the enabling systems.

6.0. Step 2: Conduct CPI and CC Identification Analysis

6.1. Step 2a: Conduct CPI Identification Analysis

Step 2a, Conduct CPI Identification Analysis (Figure B-1) is a top to bottom technical review of the program, the system under evaluation, its architectures, functional decompositions, data flows and interfaces, and technologies intended to identify candidate CPI items. Best practice is for a Systems Security Working Group (SSWG) to support the CPI Identification technical analysis effort. CPI identification results from a structured decomposition of the system into the elements that contribute to the warfighter's technical advantage. Additionally, a similar decomposition identifies the components critical to the development and sustainment of systems upon which mission assurance depends.

CPI analysis may include the platform, mission planning and maintenance support equipment and trainers, to the component level and will be dependent upon the scope of the contract. For international cooperative programs, the CPI analysis is used for Defense Exportability Features (DEF) analysis and Consequence of Compromise (CofC) analysis.

CPI Identification Analysis sets the stage for the protection scheme across many protection countermeasures, as defined in Table 2.2-1 of the system's PPP document. CPI identification requires robust technical analysis using system architecture diagrams, functional decomposition of the system(s), and identification of data flows when the system is functioning and where the CPI resides during different system states (e.g., power-on, standby, test, power-off). This ensures that identified CPI is protected always and during all states.

> NOTE 1: The technical analysis may include review of company proprietary designs and processes. The designation of a contractor's/sub-contractors and vendor's data, drawings, product and services as "Proprietary" are guided by DoDI 5010.44. The designation of an item being company proprietary is an input to the technical analysis conducted in support of CPI Identification, but does not necessarily determine whether the item is CPI. Similarly, the security classification of an item is an input to the technical analysis conducted in support of CPI Identification, but does not necessarily determine whether the item is CPI. "CPI should emphasize the 'crown jewels' of U.S. warfighting capability and not include all classified or sensitive information." [8].
>
> NOTE 2: The intent of Step 2a is to identify information (hardware, technology, algorithms, software, firmware, etc.) that is CPI. The focus should remain on identifying CPI without regard to mitigations.
>
> NOTE 3: For DCS, contractors identify candidate CPI to their sponsoring service, or the approving authority for CPI Lists, AFRL/CC, unless the activity is a Battlelab and Warfare Center which the approving authority is the Commander/Director" for approval.

CPI is any unique or sensitive technology that contributes to U.S. warfighters' technical advantage and provides mission-essential capability. If CPI is compromised, this could undermine U.S. military superiority. CPI may reside in software, hardware, training equipment, and maintenance support equipment.

CPI is to be identified and protected across all DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, excess defense article transfers, and any other export in which CPI is resident within the end item. It is critical to identify technologies and capabilities needing protection from discovery, exploitation, unauthorized use, and reverse engineering. CPI will be identified early and reassessed throughout the research, development, test and evaluation lifecycle of a program so that CPI protection requirements and countermeasures may be identified and applied as the CPI is developed and modified throughout the lifecycle as needed. Furthermore, CPI will be horizontally identified and protected to ensure equivalent protections are consistently and efficiently applied across programs based on the exposure of the system, consequence of compromise, and assessed threats. When identifying CPI within a system, the system should be decomposed as far as needed until the entire element/component constitutes CPI. This allows for the best horizontal protection.

Initial CPI must be identified as soon as system solutions are being traded, at the conceptual level of design, preferably in the S&T phase, or perhaps as late as TMRR. Early CPI identification drives protection requirements, which must be included in the program baseline early enough to affect programming and budgeting. CPI analysis is repeated throughout the lifecycle, from S&T through TMRR, EMD, production, and sustainment (including technology insertion and P3I).

Methods for CPI Identification include Expert Opinion, List, and Question methods. Expert Opinion methods involve those Subject Matter Experts (SMEs) who are closest to the technology, as well as, the contractor Chief Engineer (CE) and possibly contractor Lead Systems Engineer (LSE). List methods involve consulting the CPI Horizontal Protection Guidance, DoDI S-5200.39, provisos, contractor CPI databases, SCGs, etc. These sources are detailed in the "DoD AT Desk Reference," and should be emphasized early in a program. The rest of this guide describes the Question method.

Documentation is critical to CPI analysis. It should include the list of candidate CPI, source (DoDI S-5200.39, expert opinion, CPI HPG, etc), location within the system (which may require additional classification; see the AT SCG); sensitivity; contractor POC (person closest to the technology, or most knowledgeable about the technology), whether the candidate is "technology described in DoDI S-5200.39" (required for export license applications), whether the CPI meets or breaks DoDI S-5200.39 thresholds, and the rationale for why it was selected. Similarly, a list of candidate CPI "considered but rejected" should include rationale for why the candidate was rejected (i.e., COTS, publically available, etc.). A candidate CPI Watch list should document any potential CPI that require additional analysis, or for system elements that are uncertain to be in the baseline at that time in the CPI analysis.

Once a candidate set of CPI is identified, each item is then further analyzed to determine if the item is considered CPI. After the CPI list is generated, the CPI type is determined. There are two types of CPI: Organic and Inherited.

- Organic – A CPI originating in the acquisition activity either through development or integration of commercial or Government components. In other words, the CPI is owned by the program.
- Inherited – A CPI defined and owned by another program, but incorporated into your program/system.

After the candidate CPI is identified, including its type, the consequence of compromise and sensitivity of the CPI needs to be assessed in accordance with the DoD Anti-Tamper (AT) Technical Implementation Guide (TIG).

The CPI Identification analysis is described in this Section with each task containing a short summary of its purpose followed by detailed description(s) of potential inputs (depends on the life cycle phase), guidance, and outcomes. Traceability is maintained across all levels of the structured technical analysis. Several useful resources, described below, are available to assist with the CPI identification analysis.

CPI Tools and Resources.

Many sources, tools, and methods are available in support of CPI Identification Analysis (e.g., Air Force Pamphlet [AFPAM] 63-113 [7]; Figure A8.1, CPI Identification Decision Aid; Defense Acquisition Guidebook Chapter 9; CPI Horizontal Protection Guidance; Acquisition Security Database (ASDB); policy documents (i.e., DoDM S-5230.28); SCGs; review of provisos). All tools and resources aid a program in ensuring the right level of rigor and analysis of their system is applied to ensure CPI has been effectively identified. It is important to note this is a technical analysis that requires the participation of personnel with the correct level of program understanding to adequately conduct the analysis. This is not a checklist process as there is significant technical analysis that must be done to identify CPI.

Other service tools can be used for joint programs, such as the "DON CPI Tool", ARTPC Assessment Tool (facilitated by ARTPC, not a stand-alone process), and MDA 5200.08-M, Encl. 3. The "DoD CPI/CT Tool" and the Military Critical Technology List (MCTL) are obsolete, and shall not be used—they are not based on the same definition of CPI as DoDI 5200.39, and may give misleading results.

CPI analysis should include a Low Observable (LO)/Counter Low Observable (CLO) analysis (evaluation of technologies with DoDM S-5230.28) early in the process. Technologies that meet DoDM S-5230.28 thresholds, that are not COTS, are strong candidates for CPI, so LO/CLO analysis becomes a feeder to the remaining CPI analysis.

Prior to beginning the CPI Identification analysis (links provided where available), there are several helpful resources that should be reviewed; see Section **Error! Reference source not found.** for a list of CPI resources and Section **Error! Reference source not found.** for related policy and PPP references. To assist in the actual CPI Identification analysis, the following resources providing detailed technical input are available (links provided where available):

- DoD Anti-Tamper Executive Agent (ATEA) Program Office website. **https://at.dod.mil**
- DoD CPI Horizontal Protection Guidance – available from the DoD ATEA Program Office. The guide is classified Secret and should be used in conjunction with other resources in the development of candidate CPI.
- Export License Provisos – FMS or DCS cases may have provisos, export restrictions, or other types of restrictions that will need to be evaluated for CPI items. "Any export license provisos that list specific warfighting capabilities that shall not be released are possible CPI candidates, subject to the definition of CPI." [8]

- Acquisition Security Database (ASDB) – facilitates horizontal protection and provides CPI examples. The ASDB is accessible via the SECRET Internet Protocol Router Network (SIPRNet).[32]
- CPI Identification Decision Aid (AFPAM 63-113, Figure A8.1) – provides a series of questions to assist programs with their critical thinking. As each question set in the Decision Aid is associated with a different Step 2a task, programs can refer to the related set when executing each task.
- CPI Identification Survey Tool (AFPAM 63-113, Attachment 8) – provides several questions to assist programs with their critical thinking.
- DoDM S-5230.28: Low Observable (LO) and Counter Low Observable (CLO) Programs Manual (U) [9] – Programs must review this classified policy to ensure that the program does not trigger any LO/CLO thresholds.
- DoD AT Desk Reference

  NOTE 1: The intent of Step 2a is to identify information (hardware, technologies, algorithms, software, firmware, etc.) that is CPI. The focus should remain on identifying CPI without regard to mitigations.

  NOTE 2: DCS programs can use all of the same tools listed above. DCS cases should contact the ATEA on the proper approval processes for determining CPI.

6.1.1. Step 2a, Task 1: Analyze the System's Concept

Summary: The principle objective of this task is to determine if the system's concept provides an enhanced[33] or technologically advanced warfighter capability that requires additional protection. A system's concept is the description of a proposed system's characteristics in terms of the needs it will fulfill from a User's perspective. Concept development takes place early in the SE life cycle so SSWG members should be active participants in this activity.

Potential Inputs:

- AP.
- AoA.
- CONOPS.
- Critical Technology Elements (CTEs).
- Initial Concept Design Review (ICDR).
- IS-ICD/IS-CDD.

[32] https://www.dodtechipedia.smil.mil/ASDB

[33] For purposes of these tasks, *enhanced capability* is defined as "Information, technology or capability where there is implied or actual U.S. advantage over a majority of like foreign military or commercial systems (e.g., State-of-the-Art vs. State-of-the-World)."

- KPPs/KSAs.
- Operations Security Plan.
- SCG.
- VOLT.
- SEP.
- Technology Development Strategy (TDS).
- Trade Studies.
- Technical Studies/Technical Analyses.
- Alternative Systems Review materials.
- Overview and Summary Information (AV-1).
- High Level Operational Concept Graphic (OV-1).
- Operational Activity Decomposition Tree (OV-5a).

Outcome:

- List of candidate CPI.

Guidance:

Discuss the following aspects associated with the system's concept to determine whether the item should be added to the candidate CPI list.

Task 1.1: Determine if the concept is in the public domain.

Task 1.2: Determine whether divulging U.S. intent to pursue the concept would cause a public outcry or diplomatic harm.

Task 1.3: Determine whether other countries, academia, or businesses are pursuing the same or a similar technology.

Task 1.4: If other countries are pursuing the same or a similar technology, determine whether they are allies or adversaries.

Task 1.5: Determine if the development of the concept would lead to a capability.

Task 1.6: Determine whether disclosure of the concept itself enables an adversary to counter or defeat the system capability directly.

Task 1.7: Consider whether the relationship between the system and its using organization reveals details of the system or organization (otherwise not releasable).

6.1.2. Step 2a, Task 2: Analyze the System's Materials

Summary: The principle objective of this task is to determine if the system's materials or software provide an enhanced capability that requires additional protection. Materials include, but are not limited to, raw and processed material, parts, components, assemblies, fuels, and other items that may be worked into a more finished form in performance of a contract. A system's material can include the following items (note that the exact definition of these terms may be found in the Federal Acquisition Regulation, Part 2, Definitions of Words and Terms):

- *Commercial items* – "Any item that is of a type customarily used by the general public or non-Governmental entities for purposes other than Governmental purposes." Commercial items also include any commercial technologies with military application.
- *Non-Developmental Items (NDIs)* – Includes "Any previously developed item of supply used exclusively for Governmental purposes by a Federal agency, a State or local Government, or a foreign Government with which the United States has a mutual defense cooperation agreement."
- *Commercial off-the-Shelf (COTS)* – A commercial item, sold in substantial quantity in the commercial marketplace, that is offered to the Government without modification.

Potential Inputs:

- AP.
- AS.
- BOM.
- CONOPS.
- IS-ICD/IS-CDD.
- Initial Product Baseline.
- KMP.
- LCSP.
- Market Research.
- PBAs.
- PSS.
- SCG.
- SDD.
- SEP.
- SSDD.
- TDS.
- WBS.

Potential Inputs (continued):

- PDR materials.
- CDR materials.
- Systems Technology and Skills Forecast (SV-9).

Outcome:

- List of candidate CPI.

Guidance:

Discuss the following aspects associated with the system's materials and software to determine whether the item should be added to the candidate CPI list.

Task 2.1: Consider whether the system's materials, computer languages, or devices are significantly innovative or reflective of a normal upgrade.

Task 2.2: Consider whether the system's materials, computer languages, or devices provide a significantly enhanced capability or whether they make the existing capability slightly better.

Task 2.3: Determine whether the system requires development of new or modified algorithms or computer languages.

Task 2.4: Determine whether the system incorporates exotic materials or rare earth elements that are subject to export controls.

Task 2.5: Determine whether the use of exotic materials (as applied to the system) provides the system's core capability.

6.1.3. Step 2a, Task 3: Analyze the System's Design

Summary: The principle objective of this task is to determine if the system's design provides a technological advantage or if its loss would reveal the operational effectiveness of DoD capability. A system's design is comprised of elements, such as the architecture, modules, and components; the different interfaces of those components; and the data that goes through the system. The SSWG leverages the system's functional architecture and decomposes those functions into a physical architecture (a set of product, system, and/or software elements) to determine if any of the design factors may require additional protection.

Potential Inputs:

- CI and sub-CI specifications.
- IS-ICD/IS-CDD.
- ISP.
- KMP.
- Risk Management Plan (RMP).
- SCG.
- SDD.
- System architecture.
- System specification/subsystem specification.
- SEP.
- SRD.
- SSDD.
- WBS.
- PDR materials.
- CDR materials.
- Interface Control Document.
- IDD.
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).

Outcome:

- List of candidate CPI.

<u>Guidance:</u>

Discuss the following aspects associated with the system's design to determine whether the item should be added to the candidate CPI list. For each item being considered, begin the discussion with the following question: "What is the function of the item being assessed?"

Task 3.1: Determine whether the realization of this capability requires significant hardware development or modifications.

Task 3.2: Determine whether the realization of this capability requires significant software/firmware development or modifications.

Task 3.3: Determine whether loss or compromise of the design (to include Intellectual Property) would provide an adversary with a technological advantage.

Task 3.4: Determine whether compromise of the design would result in technology transfer that the adversary can leverage or use to bolster its warfighting capability.

Task 3.5: Determine whether compromise of the design would result in technology transfer that the adversary can use to counter U.S. capabilities based on weaknesses or patterns identified in the transferred technology.

Task 3.6: Determine whether this hardware/software/firmware design (either end product or engineering documentation) provides details of an exploitable system vulnerability.

Task 3.7: Compare this capability with legacy or foreign systems of similar design.

Task 3.8: Determine whether the system is designed to specifically exploit a known foreign vulnerability (hardware, software, firmware, or procedural).

6.1.4. Step 2a, Task 4: Analyze the System's Manufacturing Processes

Summary: The principle objective of this task is to determine if the system's manufacturing, fabrication and/or coding processes provide an enhanced system capability that requires additional protection. This may include unique or one-of-a-kind software capabilities, manufacturing technologies, and/or specialized suppliers, facilities, or tooling.

Potential Inputs:

- CI and sub-CI specifications.
- IS-ICD/IS-CDD.
- KMP.
- Manufacturing Maturation Plan.
- Manufacturing Readiness Assessment.
- RMP.
- SCG.
- SDD.
- System architecture.
- System specification/Subsystem specification.
- SEP.
- SSDD.
- TOs.
- PDR materials.
- CDR materials.

Outcome:

- List of candidate CPI.

Guidance:

Discuss the following aspects associated with the system's manufacturing process to determine whether the item should be added to the candidate CPI list.

Task 4.1: Identify whether the manufacturing/fabrication/coding processes are standard and/or well known.

Task 4.2: Identify whether any manufacturing processes (i.e., fabrication, tooling, calibration, coating, coding, etc.) provide a capability not otherwise inherent in the hardware, software, or firmware.

Task 4.3: Identify whether any manufacturing processes require or reveal unique tooling or materials.

Task 4.4: Identify whether the manufacturing process is classified or proprietary.

Task 4.5: Identify whether any manufacturing process was specifically customized to meet critical U.S. defense needs or technological advantage.

6.1.5. Step 2a, Task 5: Analyze the System's Integration

Summary: The principle objective of this task is to determine if the system's integration provides any unique or enhanced system capabilities that may require additional protection. There are different forms of integration. *Vertical* integration is when the components of a system, developed by a single acquisition program, are integrated to produce the desired capability. *Horizontal* integration creates new capabilities across individual systems developed by different acquisition programs.

Potential Inputs:

- CI and sub-CI specifications.
- IS-ICD/IS-CDD.
- Interface Requirements Documents/Specifications.
- ISP.
- KMP.
- SCG.
- SDD.
- SDP.
- System architecture.
- System specification/Subsystem specification.
- SSDD.
- SEP.
- TEMP.
- PDR materials.
- CDR materials.
- Interface Control Document.
- IDD.
- Systems Interface Description (SV-1).

Outcome:

- List of candidate CPI.

Guidance:

Discuss the following aspects associated with the system's integration to determine whether the item should be added to the candidate CPI list.

Task 5.1: Determine whether the integration of this item requires a significant investment in design and testing.

Task 5.2: Determine whether the integration itself (with either COTS or GOTS components) results in a new or enhanced capability.

Task 5.3: Describe how this capability compares to other U.S., commercial, or foreign systems.

Task 5.4: Determine whether this hardware/software/firmware integration effort (including supporting documentation) provides details of an exploitable system vulnerability.

Task 5.5: Determine whether loss of the integration details enable an adversary to accelerate their development effort(s). If the system is a collection of COTS parts, none of which is CPI, consider whether an adversary would be able to copy the system and realize a capability at low cost.

6.1.6. Step 2a, Task 6: Analyze the System's Operational Environment

Summary: The principle objective of this task is to determine if the system's operational environment enables an adversary to degrade the system's operational capability through a specific threat vector or increases the threat likelihood of a threat vector or vectors. If so, additional protection is warranted.

Potential Inputs:

- CONOPS.
- FMEA.
- IS-ICD/IS-CDD.
- KMP.
- SCG.
- SSDD.
- SEP.
- TRA.
- TEMP.
- Threat Documentation (e.g., VOLT).
- PDR materials.
- CDR materials.
- Systems Interface Description (SV-1).
- Capability to Operational Activities Mapping (CV-6).

Outcome:

- List of candidate CPI.

Guidance:

Discuss the following aspects associated with the operational environment to determine whether the item should be added to the candidate CPI list.

Task 6.1: Determine whether loss of this item to an adversary would enable them to develop new or enhance current counter tactics, techniques and procedures.

Task 6.2: Determine whether loss of this item to an adversary would enable them to exploit a system vulnerability, especially with regard to vulnerabilities to Electronic Attack (EA) where Electronic Protection (EP) is a system requirement.

Task 6.3: Determine whether loss of this item to an adversary would enable them to accelerate their development effort(s).

Task 6.4: Determine whether any elements associated with the system's interoperability capabilities necessitate additional protection to maintain US technological advantage.

Task 6.5: Determine whether any elements associated with the system's interoperability capabilities decrease the system's security posture.

6.1.7. Step 2a, Task 7: Compile Core Candidate CPI List

Summary: The result of the technical analysis used to identify CPI must be well documented so that a program can fully explain why each CPI item was captured and considered as a candidate CPI, or why the program has determined that there is no CPI. Candidate CPI items consist of all items the program believes could be CPI, but require additional research and analysis before a final determination is made. For example, by following this process, a program may, on the first cut, identify 100 candidate CPI items. The list is then further analyzed and refined, resulting in a distilled list of core candidate CPI items. The resulting core candidate CPI list is the foundation for what may become the program's finalized CPI list.

NOTE: This table is SECRET minimum when filled in per the AT SCG. CPI COC, for example, is SECRET.

Specific task outcomes and supporting information can be organized and captured in template form, similar to that suggested by the template in Table B-2.

Table B-1 Candidate CPI List (Template)

Function/Capability (CPI Name)	CPI Description	AT Sensitivity	Consequence of Compromise	Protection Rationale
		Modification, Sight, Existence, or N/A	Low, Moderate, or High	Examples: Countermeasure Development, Vulnerability Exploitation, Indigenous Development, Proviso Limitation

NOTE: The CPI List should be marked FOR OFFICIAL USE ONLY as a minimum, per the AT SCG. Any document that supports AT processes should be marked FOUO.

Additional columns of Table B-2 could contain:

- CPI ID Source/Method - (HPG, TIG, DoDM S-5230.28, SCG(s), Provisos, Inherited CPI List, CPI Conventions, Expert Opinion, PPP, ASDB)
- CPI Type – (organic or inherited)
- CPI location – (where is the CPI located in the system?)
- Technical POC – (who is most knowledgeable regarding this CPI)
- Technology Described in DoDM S-5230.28 (for LO/CLO analysis)
- Meets DoDM S-5230.28 Threshold (for LO/CLO analysis)

Potential Input:

- Results of technical analyses.

Outcomes:

- Core candidate CPI list with Consequence of Compromise determined.
- Determination of no CPI.
- Determination of inherited CPI that does not require additional protection.

<u>Guidance:</u>

For each piece of core candidate CPI, programs should also document the following information:

Task 7.1: The name of the CPI should be unique and distinguishable, and as descriptive as possible.

Task 7.2: Provide a precise description of the CPI item. Ensure that the CPI item is as narrowly defined as possible. The CPI description should describe what the CPI is (e.g., an algorithm, a process, a technology, a set of data) and for what the CPI is used (i.e., its intended purpose).

Task 7.3: See the TIG or the HPG for descriptions of the AT Sensitivities

Task 7.4: See the TIG or the HPG for descriptions of the Consequence of Compromise levels

Task 7.5: See the HPG for descriptions of Protection Rationale

Task 7.6: Identify the source or method used to identify the CPI.

Task 7.7: Identify the type of CPI: organic or inherited. For inherited CPI, list the owning organizational office symbol and the point of contact or program name.

Task 7.8: Identify the residency of the CPI. Identify where the CPI resides during different phases of the system (at rest, load, execution, etc.). For example, if it resides on the space and weapon system, it would be WS-CPI1…WS-CPIX or maintenance system would be MS-CPI1..MS-CPIX.

Task 7.9: Identify where exactly the CPI is located in the system. The hardware/software should be decomposed until the entire element identified constitutes CPI.

Task 7.10: Identify a good technical point of contact who is familiar with the CPI.

CPI identification is an iterative process. The relevance and accuracy of the outcomes require the process to be executed many times across the acquisition life cycle, as more detailed information about the missions, the role of the system in supporting the missions, and the details of the system design become known. CPI identification continues through the Production and Deployment (P&D) and Operations and Sustainment (O&S) phases.

6.1.8. Step 2a, Task 8: Compile Eliminated CPI List

Summary: During the CPI identification analysis, some items will be initially considered as CPI, but will be eliminated upon further analysis. These items should be captured along with their rationale for elimination. The rationale should be substantial so that other stakeholders involved in either concurrence and/or approval will understand the completed analysis. To capture items eliminated as CPI candidates, the template provided in Table B-3 can be used.

Table B-2 CPI Items Eliminated as Candidates (Template)

CPI Name	CPI Description	CPI Type (Organic/Inherited)	Rationale	Documentation

Potential Input:

- Results of technical analyses

Outcome:

- List of CPI items eliminated as candidates

Guidance:

Compile a list of CPI items eliminated as candidates.

Task 8.1: Review the list of CPI items that were previously considered but eliminated.

Task 8.2: Record the name of the eliminated item. The name of the CPI should be unique and distinguishable, and as descriptive as possible.

Task 8.3: Provide a precise description of the CPI item. Ensure that the CPI item is as narrowly defined as possible. The CPI description should describe what the CPI is (e.g., an algorithm, a process, a technology, a set of data) and for what the CPI is used (i.e., its intended purpose).

Task 8.4: Identify the type of CPI.

Task 8.5: Provide substantial rationale and supporting documentation to back up your determination. Rationale might include CPI described in the HPG or DoDM S-5230.28, but may be COTS, or procured from foreign sources.

6.1.9. Step 2a, Task 9: Compile CPI Watch List

<u>Summary</u>: During the CPI identification analysis, some items will be initially considered as CPI, but will be eliminated upon further analysis. As the system design develops, some items that were previously eliminated may warrant monitoring to consider as possible CPI. In addition, baseline changes may lead to additional candidate CPI. A CPI watch list should be compiled and reviewed as the design develops.

Table B-4 may be used to organize and capture possible CPI items that may emerge in the future.

Table B-3 CPI Watch List (Template)

Name of Possible CPI	CPI Description

<u>Potential Inputs:</u>

- Results of technical analyses
- List of CPI items eliminated as candidates

<u>Outcome:</u>

- List of possible CPI items to watch for future review and analysis

<u>Guidance:</u>

Compile a list of CPI items that should be watched.

Task 9.1: Review the list of CPI items that were previously considered but eliminated.

Task 9.2: Determine whether any of those items may become possible CPI as the system design matures.

Task 9.3: Analyze any baseline changes that are being proposed since the last CPI identification analysis. Identify any possible CPI items in the proposed baseline.

Task 9.4: Record the name of the possible CPI. The name of the CPI should be unique and distinguishable, and as descriptive as possible.

Task 9.5: Provide a precise description of the CPI item. Ensure that the CPI item is as narrowly defined as possible. The CPI description should describe what the CPI is (e.g., an algorithm, a process, a technology, a set of data) and for what the CPI is used (i.e., its intended purpose).

Task 9.6: Review the CPI watch list during subsequent CPI identification analyses. Determine whether any possible CPI items have become candidate CPI or whether they should be removed from the watch list.

6.2. Step 2b: Conduct CC Identification Analysis

Step 2b, Conduct CC Identification Analysis (Figure B-1) is essential to building more secure systems. Identification and protection of critical components is required for applicable systems, as defined in DoDI 5200.44. Applicable systems refer to: (a) national security systems, (b) any DoD system with a high impact level for any of the three security objectives (confidentiality, integrity, and availability); (c) other DoD information systems (see the glossary for the full description).

The purpose of this process is to identify the complete set of components that execute a system's Mission Critical Functions (MCFs) and are used to build uncompromised weapons and information systems. Any design vulnerabilities in these components or a sabotage by an adversary may result in DoD's warfighting mission capabilities being impaired. The intent of this process is to compile a complete list of all CCs, across multiple environments that deliver/protect an MCF, or may introduce a design vulnerability to a required system function at any time throughout the life cycle of the system. With a complete compilation of CCs, all stakeholders' needs can be satisfied. This identification of CCs is conducted before any constraints are imposed. All components should be defined so that the program knows their entire list as any component may introduce risk.

For the TSN stakeholder, the CC Identification Process described in this Section will satisfy the requirement to perform a criticality analysis. Refer to the Defense Acquisition Guidebook, [11], Chapter 9 for the following: *"The criticality analysis allows a program to focus attention and resources on the system capabilities, mission critical functions, and critical components that matter most. Mission critical functions are those functions of the system that, if corrupted or disabled, would likely lead to mission failure or degradation. Mission critical components are primarily the elements of the system (hardware, software, and firmware) that implement mission critical functions. It can include components that perform defensive functions that protect critical components, and components that have unobstructed access to critical components.*

Criticality analysis includes the following iterative steps:

- Identify and group the mission capabilities the system will perform.
- Identify the system's mission critical functions based on mission capabilities, and assign criticality levels to those functions.
- Map the mission critical functions to the system architecture and identify the defined system components (hardware, software, and firmware) that implement those functions (i.e., components that are critical to the mission effectiveness of the system or an interfaced network).
- Allocate criticality levels to those components that have been defined.
- Identify suppliers of critical components."

The environments to be considered include the operational environment for the system under consideration (i.e., the system-of-interest) and the environments for the enabling systems. Some examples of enabling systems include development systems, test systems, training systems, and maintenance systems.

Table B-4 Definitions for System Terms [34]

Terms	Definitions
System	Combination of interacting elements organized to achieve one or more stated purposes.
System Elements	Any combination of technology/machine, human, physical and environmental elements. The combination itself may be referred to as a system.
System-of-Interest	The bounded context that is the focus of the engineering effort. Bounds may be physical or logical.
Enabling System	System that exists in the life cycle of the System-of-Interest and supports the development, manufacture, utilization, sustainment, or life cycle activity associated with the System-of-Interest.
Other System	System that interacts with the System-of-Interest in its operational environment.
Lowest Level Element	Purchased and managed as an End-Item.

The identification of CC is performed to the level of procurement and/or at the level being managed by the program office. For example, many systems procure servers, routers, single board computers, laptops, crypto devices, and other 'higher order assemblies' above a single integrated circuit, such as an Application-Specific Integrated Circuit (ASIC) or a Field-Programmable Gate Array (FPGA). Many systems also procure integrated circuits, e.g., ASICs or FPGAs, that are designed into the system by the acquisition program and that are managed as developmental items of the program. All these items are identified as CCs when they deliver/protect MCFs, or may introduce design vulnerabilities into the system functionality during the life cycle of the system. Further, these items may be subject to notifications or recalls by the vendor when the vendor becomes aware of a vulnerability. All of these components being managed or procured by the program office should be submitted for a Threat Assessment Center (TAC) Report from the Defense Intelligence Agency (DIA) when they satisfy the criteria for identification as CCs in accordance with DoDI 5200.44.

Details of the CC Identification Process steps are described in this Section. Each step contains a short summary of its purpose followed by detailed description(s) of potential inputs (depends on the life cycle phase), guidance, and outcomes.

The CC identification results from a functional decomposition of the system-of-interest into its mission critical functions. Additionally, similar decompositions identify the CCs used in the enabling systems that are essential for the system-of-interest. The information captured serves to support execution of

[34] Adapted from ISO/IEEE 15288:2015, "Systems and Software Engineering – System Life Cycle Processes".

the entire CC Identification Process and supports life cycle engineering, trades, risk management, and the following reporting and document expectations:

- Inputs to the PPP.
- Criticality level and rationale.
- Supplier information to support the DIA TAC RFI.

CC identification is an iterative process. The relevance and accuracy of the outcomes require the process to be executed many times across the acquisition life cycle, as more detailed information about the missions, the role of the system in supporting the missions, and the details of the system design become known.

CC identification continues through the P&D and O&S phases. At the Physical Configuration Audit and Full Rate Production (FRP)/Full Deployment Decision (FDD) points CCs can be identified at the BOM level based on the established Configuration Product Baseline.

6.2.1. Step 2b, Task 1: Identify and Group the System's Mission Capabilities

Summary: An understanding of the system's mission capabilities will provide the foundation for a comprehensive approach to identifying the underlying components.

Potential Inputs:

- CONOPS.
- IS-ICD/IS-CDD.
- SRD.
- Use Cases.
- Operational Resource Flow Matrix (OV-3).
- Operational Activity Decomposition Tree (OV-5a).
- Operational Activity Model (OV-5b).
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).
- Operational Activity to Systems Function Traceability Matrix (SV-5a).
- Operational Activity to Systems Traceability Matrix (SV-5b).

Outcome:

- Identification and grouping of the system's mission capabilities.

Guidance:

Task 1.1: Identify the mission capabilities that the system will perform. Mission SMEs identify the mission capabilities.

Task 1.2: Group the system's mission capabilities.

6.2.2. Step 2b, Task 2: Identify the System's Mission Critical Functions

<u>Summary</u>: An end-to-end functional decomposition of mission capabilities on the system-of-interest and each enabling system will be performed to identify the mission critical functions. Criticality levels will be assigned to the MCFs.

NOTE: During this step, following system safety guidance contained in MIL-STD-882, programs are highly encouraged to identify their safety critical items and safety critical functions. Safety critical functions may impinge on mission critical functions and vice versa. This understanding will inform the developer with certain design considerations and process actions to be employed because of the safety related nature and/or mission related nature of the function, where applicable. For USAF air systems, additional guidance is provided in Airworthiness Circular AC-17-01.

<u>Potential Inputs:</u>

- CONOPS.
- IS-ICD/IS-CDD.
- SRD.
- Use Cases.
- Operational Resource Flow Matrix (OV-3).
- Operational Activity Decomposition Tree (OV-5a).
- Operational Activity Model (OV-5b).
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).
- Operational Activity to Systems Function Traceability Matrix (SV-5a).
- Operational Activity to Systems Traceability Matrix (SV-5b).
- TOs, when available (Operator or Operations Manuals as another potential source).

<u>Outcome:</u>

- List of MCFs with assigned criticality levels.

Guidance:

Task 2.1: Decompose the mission capabilities of the system-of-interest and its enabling systems into their MCFs.

Task 2.2: Assign criticality levels to each MCF. This process is used to identify the MCFs based upon the likelihood of mission failure if the function is corrupted or disabled. Do not include any system elements that are outside the system boundary. Assign a criticality level for each function as follows (see [11], Chapter 9, Table 3).

- Criticality Level I – Total Mission Failure (Failure that results in total compromise of mission capability).
- Criticality Level II – Significant/Unacceptable Degradation (Failure that results in unacceptable compromise of mission capability or significant mission degradation).
- Criticality Level III – Partial/Acceptable (Failure that results in partial compromise of mission capability or partial mission degradation).
- Criticality Level IV – Negligible (Failure that results in little or no compromise of mission capability).

Task 2.3: Ensure that stakeholders agree with the criticality level assigned to each mission critical function.

6.2.3. Step 2b, Task 2: Map MCF to System Architecture & Components

Summary: Map each mission critical function to the system architecture. Trace each MCF to the hardware, software, and firmware components that implement them. Continue the decomposition until the lowest level of components procured and/or managed as end-items are identified. List the CCs designed into the system-of-interest and in each enabling system.

This task is limited to Information and Communications Technology (ICT) components. It is important to ensure that all CCs designed into the system-of-interest and each enabling system are included.

Potential Inputs:

- BOM.
- CI and sub-CI specifications.
- Data flow diagrams.
- LRU list.
- Requirements Traceability Verification Matrix.
- SSDD.
- SEP.
- System architecture.
- System specification/Subsystem specification.
- TOs.
- PDR materials.
- CDR materials.
- Interface Control Document.
- IDD.
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).
- Operational Activity to Systems Function Traceability Matrix (SV-5a).
- Operational Activity to Systems Traceability Matrix (SV-5b).
- Operational Resource Flow Matrix (OV-3).
- Operational Activity Model (OV-5b).

Outcomes:

- List of CCs for the system-of-interest.
- List of CCs for the enabling systems.

A BOM-level identification of components in a system is not likely to be known early in the ILC, such as during the Materiel Solution Analysis Phase and the Technology Maturation and Risk Reduction Phase. The complete list of system components may not be known until the decision to proceed with the P&D Phase is made.

Guidance:

Task 3.1: Map each MCF to the system architecture.

Task 3.2: Trace each MCF to the hardware, software, and firmware components that implement them.

Task 3.3: Continue the decomposition until the lowest level of components procured and/or managed as end-items are identified. Consider the following when identifying components:

- Include components that have the following characteristics:
    - ➢ Provide a path of unmediated (direct or immediate) access to a CC.
    - ➢ Are able to interfere with the behavior of a CC.
    - ➢ Provide separation of security domains.
    - ➢ Provide means for data/information to cross-security domains.
- Assess, for inclusion, those components that provide connectivity to other systems, including industrial control systems.
- Ensure that spare and replacement parts are included.

Task 3.4: List the CCs designed into the system-of-interest and in each enabling system:

- Some CCs consist of electronic components at a device level (e.g., ASICs, FPGAs, and Erasable Programmable Read-Only Memories).
- Other CCs may include higher-level assemblies, such as single board computers, laptops, servers, routers, network switches, or other assemblies that are purchased and managed as end-items.

6.2.4. Step 2b, Task 4: Allocate Criticality Levels to CCs and Identify Suppliers of CCs.

Summary: Once the list of CCs has been generated, each CC needs to be assigned a criticality level. Each program may have more than one stakeholder interested in this information. Identify the supplier information for each component.

Potential Inputs:

- BOM.
- CI and sub-CI specifications.
- Data flow diagrams.
- LRU list.
- Requirements Traceability Verification Matrix.
- SEP.
- SSDD.
- Sequence Diagrams
- Activity Diagrams
- System architecture.
- System specification/subsystem specification.
- TOs.
- PDR materials.
- CDR materials.
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).
- Operational Activity to Systems Function Traceability Matrix (SV-5a).
- Operational Activity to Systems Traceability Matrix (SV-5b).
- Operational Resource Flow Matrix (OV-3).
- Operational Activity Model (OV-5b).
- Operational State Diagrams (OV-6b)
- Systems State Transition Diagrams (SV-10b).

Outcomes:

- Criticality level assigned to each CC.
- Rationale for determining criticality level.
- Component supplier information.

<u>Guidance:</u>

Task 4.1: Criticality may be assessed in terms of the impact of function or component failure. Assign a criticality level for each CC as follows (see [11], Chapter 9, Table 3):

- Criticality Level I – Total Mission Failure (Failure that results in total compromise of mission capability).
- Criticality Level II – Significant/Unacceptable Degradation (Failure that results in unacceptable compromise of mission capability or significant mission degradation).
- Criticality Level III – Partial/Acceptable (Failure that results in partial compromise of mission capability or partial mission degradation).
- Criticality Level IV – Negligible (Failure that results in little or no compromise of mission capability).

Task 4.2: Determine which stakeholders need the complete list of CCs and which stakeholders will utilize the list of CCs according to their criticality level.

Task 4.3: Ensure that stakeholders agree with the criticality level assigned to each critical component.

Task 4.4: Identify suppliers of critical components.

- Step 3: Conduct CPI and CC Horizontal Consistency Analyses.

6.3. Step 3a: Conduct CPI Horizontal Consistency Analysis.

Horizontal Protection of CPI across the DoD is necessary to ensure that CPI associated with more than one program is protected to the same degree. If one program identifies CPI, other programs will also need to protect that CPI to the same degree. Outside of SSE, contractors may not recognize “horizontal protection,” but will understand re-use. It is in the re-use of algorithms, subsystems, components, etc., that horizontal protection can be most effectively tracked.

The ASDB offers a starting point for horizontal protection efforts. The ASDB enables DoD cross-program CPI reporting and analysis in support of horizontal protection. It also provides points of contact/CPI SMEs to facilitate CPI identification and protection discussions across Program Offices. Program use of the ASDB needs to be addressed in the PPP, Section 4.0. The ASDB is accessible via the SIPRNet and is helpful during this step.
https://www.dodtechipedia.smil.mil/ASDB

In accordance with the DoD CPI Horizontal Protection Guidance (HPG) issuing memorandum, 8 Aug 2018, the HPG is mandatory for all programs to use when identifying CPI and determining the associated AT requirements. The DoD CPI HPG fulfills the responsibility in DoDI 5230.28 to “review emerging technologies and maintain a list of CPI to ensure horizontal protection of the technologies **and** capabilities that are essential to maintaining operational advantage for U.S. warfighters.” Figure B-4 illustrates how CPI is identified, protected, and verified across the DoD services.

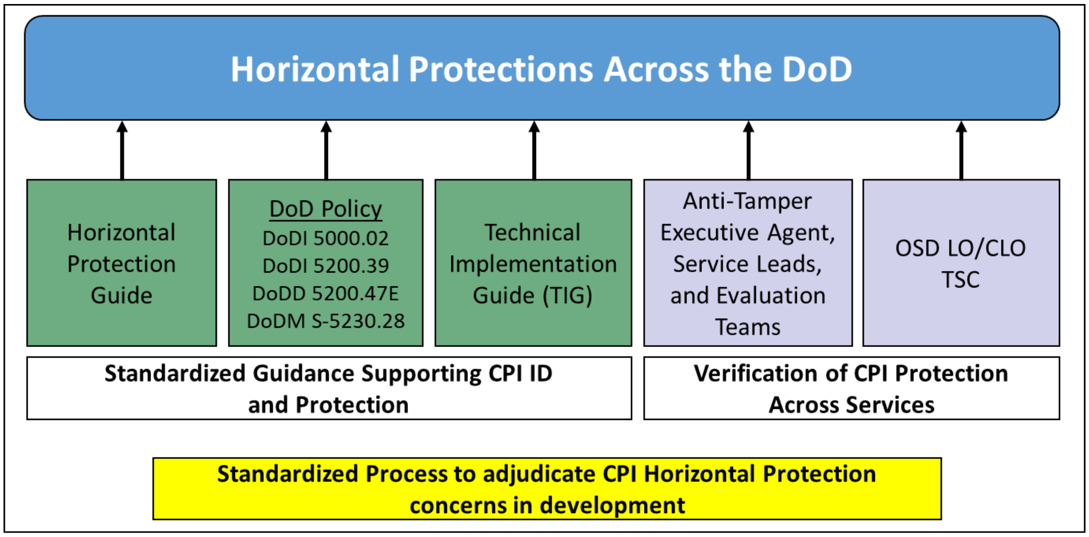

Horizontal Protections Across the DoD
Horizontal Protection Guide
DoD Policy
DoDI 5000.02
DoDI 5200.39
DoDD 5200.47E
DoDM S-5230.28
Technical Implementation Guide (TIG)
Anti-Tamper Executive Agent, Service Leads, and Evaluation Teams
OSD LO/CLO TSC
Standardized Guidance Supporting CPI ID and Protection
Verification of CPI Protection Across Services
Standardized Process to adjudicate CPI Horizontal Protection concerns in development

Figure B-4 Horizontal Protection

As a result of the CPI Horizontal Consistency Analysis, a program may either add CPI items or remove candidate CPI items from their list. If items on the candidate CPI list are no longer being considered as CPI, it is important to document this, identify who deemed that item(s) is no longer CPI (this could be in the form of a memorandum, email, policy, etc.), and explain, in short detail, why the item(s) is no longer considered to be candidate CPI. Once all remaining candidate items have been reviewed by the program, contractor, and stakeholders, the resulting set is considered the finalized CPI list.

Potential Inputs:

- Authoritative database.
- CI and sub-CI specifications.
- CONOPS.
- Data flow diagrams.
- IS-ICD, IS-CDD.
- ISP.
- KPPs and CTEs.
- LRU list.
- SDD.
- SSDD.
- SEP.
- System architecture.
- System specification/subsystem specification.
- PDR materials.
- CDR materials.
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).
- Operational Activity to Systems Function Traceability Matrix (SV-5a).
- Operational Resource Flow Matrix (OV-3).
- Operational Activity Model (OV-5b).
- Candidate CPI list.

Outcomes:

- List of the programs with same or similar CPI (if applicable).
- Adjusted consequence of compromise (CofC) assigned to each CPI with rationale (if applicable).
- Finalized CPI list.

Guidance:

Task 1.1: Query the ASDB to identify the CPI that match the CPI identified by the program. The Horizontal Consistency Analysis is informed by the CPI information contained in the ASDB. This database serves as a cross-program repository of CPI information and as a CPI knowledge base.

Task 1.2: Because of the ASDB review, a program may add CPI items or may remove candidate CPI items from their list. If items on the candidate CPI list are no longer being considered as CPI, it is important to document this, identify who deemed that item(s) is no longer CPI (this could be in the form of a memorandum, email, policy, etc.), and explain, in short detail, why the item(s) is no longer considered to be candidate CPI. Also, refer to previous content on the list of eliminated CPI and the CPI watch list.

For inherited CPI, if the program judges the CofC to be different than the originating program, coordinate with the originating program on the appropriate CofC for both systems. Differences may exist justifying the difference, or one program may need to change. Differences between services are adjudicated by the ATEA; differences within a service are adjudicated by the Service AT OPR; differences within a PEO are adjudicated by the PEO.

Task 1.3: Document the action taken, justification, and rationale for each entry made to the database. Once validated, Horizontal Protection Information will be provided in the PPP, Table 4.0-1, “Horizontal Protection Information (mandated)”.

Task 1.4: Once all remaining candidate items have been reviewed by the program and contractor, it is approved by the PM, and approved by the MDA.

6.4. Step 3b: Conduct CC Horizontal Consistency Analysis.

Conduct CC Horizontal Consistency Analysis (see Error! Reference source not found.) increases the c onsistency of CC analysis rigor across programs, leverages, and reuses the CC information and knowledge that exist across programs, and builds a comprehensive repository of information regarding CCs.

This step ensures that the identification and assessment of component criticality is consistent across PEO programs, where it is determined that equal component criticality across programs is appropriate. For the case in which a program has identified CCs and/or has assigned criticality to CCs in a manner that differs from other PEO programs, this step ensures that any differences are justified and substantiated. The outcome of this step is a program-specific determination of the identification of CCs and the assignment of criticality to CCs.

Potential Inputs:

- BOM.
- CI and sub-CI specifications.
- Data flow diagrams.
- LRU list.
- Authoritative database (Note, that the ASDB does not include CCs and cannot be used for CCs.).
- Requirements Traceability Verification Matrix.
- System architecture.
- System specification/subsystem specification.
- SEP.
- SSDD.
- TOs.
- PDR materials.
- CDR materials.
- Systems Interface Description (SV-1).
- Systems Functionality Description (SV-4).
- Operational Activity to Systems Function Traceability Matrix (SV-5a).
- Operational Resource Flow Matrix (OV-3).
- Operational Activity to Systems Traceability Matrix (SV-5b).

Outcomes:

- Updated/verified criticality level assigned to each CC.
- Rationale for updated/verified criticality level.

Guidance:

Task 2.1: Query the authoritative database to identify the CCs that match the CCs identified by the program. The Horizontal Consistency Analysis is informed by the CC information contained in the authoritative database. This database serves as a cross-program repository of CC information and as a CC knowledge base. The conduct of the Horizontal Consistency Analysis may result in alteration of the criticality assigned to a component, identification of new CCs, modification of the criticality of existing CCs, and deletion of CCs. The database entry for a CC includes rationale to substantiate selection of the same or different criticality levels across PEO programs.

Task 2.2: Determine if the criticality level assigned to the CC by the program matches that found in the database, and determine if there is a justified basis for having the same criticality level assigned. This may require the program to change their criticality level to match that found in the database, to recommend that subsequent assignments of criticality levels to that component match what the program determined to be appropriate, or to accept the difference in the assigned criticality level as being justified.

Task 2.4: Document the action taken, justification, and rationale for each entry made to the database. Update the authoritative database to reflect decisions made.

6.5. Step 4: Conduct Non-Advocate Review (NAR) for CPI and CC.

Following the CPI and CC Horizontal Consistency Analysis and review, many programs conduct a Non-Advocate Review (NAR). This is an optional step that numerous PEOs and programs have found to be beneficial as the NAR ensures that engineering rigor has been applied in the CPI and/or CC identification analyses. The Non-Advocate Review is a recommended best practice. The purpose of the NAR is to have an independent view by a team of knowledgeable SMEs who may generate questions for programs to consider ensuring that they have analyzed all applicable areas in their technical analysis.

> **NOTE:** The roles identified in the NAR process below provide general guidelines, but the specific roles may not apply to your PEO. In that case, the roles should be tailored to the organizational structure and responsibilities that pertain to your PEO.

A CPI Non-Advocate Review provides the Program Manager with an independent review, assessment, confirmation, and recommendations about the list of CPI and about the assigned criticality levels. The CPI NAR assists in ensuring that the expected rigor has been applied to the CPI Identification Analysis and the Consequence of Compromise (COC) Level Analysis, as well as, affords the PM and staff an opportunity to capitalize on outside knowledge and experience. The CPI NAR is similar in concept to an ASP's review of program management strategies. This step also provides the chain of command for SSE with a level of confidence about the program's accuracy and completeness in identifying CPI and determining the criticality levels and horizontal protection concerns.

Ideally, the CPI NAR Team would consist of SMEs external to the Program Office who are familiar with the technologies in use, the space and weapon system type, and the AT process. This NAR would inform the program with the "view of others" and assist in normalizing the identification process, educating and training the participants, and increasing cross-program information flow across USAF and PEO programs.

A CC Non-Advocate Review provides the PM with an independent review, assessment, confirmation, and recommendations about the components identified as CCs and the criticality assigned to the CC. This step also provides the chain of command responsible for SSE with a level of confidence about the program's accuracy and completeness in identifying CCs and in determining the criticality of each CC. NARs are helpful when programs are suspected of not performing due diligence in order to minimize CPI and costs. They can be held by the contractor, as well as, the Government. If the PM is driving a no-CPI determination, the NAR should report to the PEO or AT Service OPR.

If both the CPI and CC identification analyses are conducted, a combined CPI/CC NAR may be conducted whereby both the list of CPI and components identified as CCs are reviewed.

<u>NAR Objective:</u>

The objective of the NAR is to provide an independent review and assessment of the CPI/CC identified by the program and of the criticality level assigned to each CC and the consequence of compromise assigned to each CPI. The NAR serves as a program-independent means to ensure due diligence and rigor in scoping and conducting the technical analyses outlined in Steps 2 and 3, and readiness to proceed to Step 5. The NAR Team is not authorized to "approve" or "disapprove" a program's identification of CPI/CC. The results of the NAR may require programs to revisit their analyses or conduct additional analyses.

Types of NARs:

Two types of CPI/CC NARs can be conducted: informal and formal:

1. Informal – An informal NAR is provided in a small group environment with program staff to informally discuss the process used to gather and identify the candidate CPI items and/or to informally discuss the process used to gather and identify the CC items. An informal NAR is usually conducted by the PEO SSE Lead. Recommendations may be made to the program as far as their rigor and suggestions on how to further refine their list. Informal NARs are conducted at the request of the programs.

2. Formal – The purpose of the formal NAR is for a program to receive an independent (i.e., outside the program) review of their finalized CPI/CC list. The analysis is to be completed by a small team consisting of SMEs from the technologies in use, and the space and weapon system type. It is recommended that the prime contractor be present, as well as, others involved in the chain of command for SSE. The formal NAR also presents an opportunity for the involvement of external stakeholders to participate, (e.g., the Anti-Tamper Executive Agent may be involved in the CPI Identification Process.) The formal NAR is conducted by reviewing the NAR template and having the program walk through its analysis and decision-making process. The results of the NAR are then documented in meeting minutes that are used not only for reference in the to-be prepared CPI Staff Summary Sheet (SSS) and/or CC SSS, but also as an educational aid for future programs. The NAR template also provides the formats and data that are reused in the rest of the program protection planning process.

Formal NAR Team Composition – The CC NAR Team is a combination of Government and Contractor personnel that are external to the program being reviewed. The recommended makeup of the CC NAR Team is as follows:

- A chairperson: The Division SSE Lead or a designee from the PEO Office.
- Three to five SMEs on the technologies in use and the type of system being acquired from across the Directorate, who are outside the program in review.
- Procurement and logistics process representatives.
- Contractor personnel with engineering, development, and integration background.
- Identification of CPI and the assigned consequence of compromise.

The NAR is supported by Program Office SMEs who are available to answer questions during the conduct of the NAR. The PM, LE, and others involved in the chain of command for SSE are expected to participate.

Formal NAR Planning – The NAR Team coordinates with the Division SSE Lead in advance of conducting the NAR. Planning considerations include the following actions:

- Determine the length of the NAR.
- Identify the attendees and their availability.
- Schedule the NAR with the Division SSE Lead.
- Establish the date, time, place, and meeting logistics.
- Generate the NAR read-ahead materials.
- Distribute the NAR read-ahead materials one week prior to the NAR being held to participants for their review.
- Conduct the NAR.
- Record the minutes and action items.
- Assign and resolve action items.
- Perform the NAR closeout.

The NAR is a short, focused, independent review that nominally requires three days. One day is for conducting the NAR, and that time is tailored to match the amount of material to be covered. One additional day is planned for read-ahead time prior to the NAR, and the third day is dedicated to the NAR Team briefing the results.

The read-ahead time is intended to provide all NAR participants with preparation time; it is expected that all participants come to the NAR fully prepared to discuss, within their area of expertise: (a) the identification of CPI and the assignment of a consequence of compromise to each CPI and/or (b) the identification of CCs and the assignment of a criticality level to each CC.

The program should recognize that the NAR is an Engineering/Technical review that is focused on the technical rigor, accuracy, and completeness of the activities that determine CPI and on conducting a horizontal consistency check and/or the activities that determine component criticality and conduct horizontal consistency. The NAR is not the venue to address program issues and/or differences of opinion within the program on the list of CPI and/or opinion on the assignment of criticality to components. Those issues should be resolved to the extent possible prior to the NAR.

Formal NAR Scheduling – If the program is ready to proceed, the following steps should be conducted:

- Determine the length of the NAR – depends on how much material needs to be covered. The main point is to coordinate the availability of all the right SME's attendance with the NAR Team.
- Coordinate the SMEs and attendees, and determine their availability. Each SSE/AT Lead will be able to identify the SMEs from across their Directorates that are available to participate.
- Schedule the NAR with the PEO SSE/AT Lead(s).
- Secure a classified room, if necessary, and ensure that NAR members have sufficient notice to send clearance information, when required.
- Prior to the NAR, send out the NAR materials to participants for their review, which should be done one week prior to the meeting date.

Formal NAR Documentation and Template – A NAR Briefing template reflecting the combined CPI/CC Identification Process has been developed to assist programs in capturing the correct level of detail. The briefing slides are used whether the program is undertaking the combined CPI/CC Identification Process, the CPI Identification Process only, or the CC Identification Process only.

The three-part template includes two parts that are applicable to CPI NARs. The first part is called the NAR Program Description (Part 1). This part identifies information about the program, such as the program description, status, etc., and is generally unclassified, but is subject to the program's own Security Classification Guide. The second part is called the CPI NAR Program Specifics (Part 2). This part identifies the program specifics and is usually populated on the SIPRNet. This part is classified and is subject to the AT Classification guide, in addition to the program's SCG

- The three-part template includes two parts that are applicable to CC NARs. The first part is called the NAR Program Description (Part 1). This part identifies information about the program, such as the program description, status, etc., and is generally unclassified, but is subject to the program's own Security Classification Guide. The other part is called the CC NAR Program Specifics (Part 3). This part is usually unclassified, but is subject to the program's SCG.

Formal NAR Conduct – The actual NAR meeting is generally no more than two to three hours in length. The NAR Team should include the development contractors, or the contractor(s) should at least have reviewed and concurred on the program's CPI list and/or CC list prior to the CPI NAR conduct. Program SMEs will be available in real time to address any questions associated with the CPI and/or CCs in their areas (e.g., Mission Systems SMEs, Sensor SMEs, specialty SMEs).

The program may invite observers if they wish. However, the program should keep in mind that this is an Engineering/Technical review that is focused on the technical rigor of the CPI and/or CC Identification Processes, criticality levels/consequence of compromise, and horizontal protection concerns. The NAR Team will provide the PM and other designated personnel with a report within three business days of the NAR conduct, if not documented in real time as part of the meeting minutes.

Upon completion of the formal NAR, programs may have action items that need to be revisited, or they may be ready to prepare for formal submission to the PEO.

Formal NAR Out Brief – The NAR Team performs the following actions:

- Identifies and explains gap areas that the program should resolve.
- Provides recommendations and assists the program in determining the course of action to address gaps.
- Offers considerations and guidance for inclusion of additional information and rationale that supports the:
- Identification of CPI and the assigned consequence of compromise.
- Identification of CCs and the criticality level assigned to components.
- Provides process improvement recommendations.

7.0. Step 5: Submit and Obtain Approval for CPI and CC.

The PEO prepares the package of CPI and CC determinations for PEO staffing. Section 2.8.2 of AFPAM 63-113 [7] states that the MDA "validates CPI determinations, critical component determinations, and program protection approach when approving PPPs." However, for Nuclear Weapon Systems, AFSEC/SEW is the approving authority. For Space Systems, it is SMC as the approving authority.

7.1. Prepare CPI Package.

The program prepares an SSS to be used to coordinate the Program CPI list with the PEO (or his/her designee). The PEO Staffing Package includes the SSS and the following four tab attachments (possibly five tab attachments, if applicable):

- Tab 1 - Finalized CPI List: Comprised of information generated during the execution of all steps of the CPI Identification Process. Include any LO/CLO equities subject to the LO/CLO SCG and, for export, the Tri-Service Committee.
- Tab 2 - CPI Identification Analysis Write-Up: A prose description of the program's CPI Identification Analysis conducted to reach their CPI determination.
- Tab 3 - Completed CPI NAR Briefing (if conducted): Includes the completed CPI NAR Briefings (Parts 1 and 2).
- Tab 4 - Completed CPI NAR Minutes (if conducted): Includes the minutes from both CPI NAR Briefings (Parts 1 and 2). These minutes should include a description of any action items, the organization/individual responsible for the action, and the action completion status.
- Tab 5 - If applicable, attach any ITAR restrictions or provisos identifying restrictions.

Other signature requirements are dependent on the specific PEO. In addition, programs need to submit an Integrated Threat Assessment (ITA) request on their CPI to the AF Office of Special Investigations (AFOSI) by filling out an ITA form. It is important to note that *programs should not wait for the results of the ITA* before completing their Staffing Package. Once the ITA is completed, programs can then use the data received to make decisions on how to build their future mitigation strategies. The outcome of this step is the completed PEO Staffing Package with the SSS, associated tab attachments, and the separately submitted ITA.

For those programs with a No CPI determination, a No CPI Memorandum [12] should be completed and submitted with the program's signed PEO Staffing Package, which constitutes the CPI assessment (mentioned in the memorandum) to the USAF AT Deputy. (The PEO AT Lead or designee would be the approver identified in Paragraph 1 in the memorandum.)

All memoranda should be coordinated through the designated Division SSE Lead prior to the CPI NAR being conducted. Once the CPI SSS has been coordinated and has been signed, an electronic copy of the PEO Staffing Package should be provided to the Division SSE Lead, who will then transmit the completed memorandum and CPI Staffing Package to the USAF AT point of contact, copying the PEO AT Lead.

If the CPI Staffing Package contains a classified document, then the entire package should be sent via the SIPRNet; alternatively, if there are no classified documents in the CPI Staffing Package, then the package can be sent via unclassified channels.

NOTE: The No CPI determination is not a one-time, permanent "waiver" for a program. The CPI analysis is a living review that should be updated at each configuration change, so if CPI is added (via a modification, configuration change, etc.), then it must be captured and documented at that time.

7.2. Prepare CC Package.

The program prepares an SSS to be used to coordinate the Program CC list with the PEO (or his/her designee). Concurrences from the PEO on the identification of CCs, the criticality level assigned to each CC, and the list of CCs to be (or already) submitted for DIA TAC assessment are requested.

The PEO Staffing Package includes the SSS and the following four tab attachments:

- Tab 1 - Program CC List: Comprised of information generated during the execution of all steps of the CC
  Identification Process. The information for each CC may not be at the same level of specificity. This reflects what might be known at some point in the engineering process, but before the BOM details of all CCs are available.
- Tab 2 - Description of Analyses to Determine Component Criticality: A narrative discussion that provides the details of the technical analyses performed during execution of this process to identify CCs and to assign criticality levels to CCs.
- Tab 3 - CC NAR Briefings (if conducted): Includes the completed CC NAR Briefing (Parts 1 and 3).
- Tab 4 - CC NAR Minutes (if conducted): Includes the minutes from both CC NAR Briefings (Parts 1 and 3). These minutes should include a description of any action items, the organization/individual responsible for the action, and the action completion status.

The outcome of this step is the completed PEO Staffing Package, which includes the SSS with the associated tab attachments.

7.3. Step 6: Update PPP and Obtain Approval of CPI & CC Determinations.

After PEO concurrence is received on the CPI and CC determinations, the system's PPP document is updated with the appropriate information (see **Figure B-4 Horizontal Protection**). The MDA approves the CPI and CC determinations when the PPP is approved.

7.4. Step 6a: Update Knowledge Repository with Final CPI and CC Lists.

The validated CPI is captured/tracked to ensure horizontal consistency across PEO programs. This step is intended to capture all relevant information about the CPI and the consequence of compromise assigned to the CPI. The information and knowledge about CPI and the assigned criticality levels that result from the execution of this process are key to the accurate horizontal protection and consistent storage/tracking of CPI. The information supports life cycle SE activities, in addition to being a basis for program protection planning. This step can be accomplished via an entry into an authoritative database (e.g., PEO CPI database, ASDB). Entry into the ASDB ensures consistent protection mechanisms across USAF and DoD programs. The outcome of this step is the updated authoritative database with validated CPI to ensure horizontal consistency across a program, PEO, the USAF, and the DoD.

The validated CC with all relevant information about components and the criticality assigned to components is captured. The information and knowledge about CCs and the assigned criticality levels that result from execution of this process are key to the accurate horizontal protection and consistent storage/tracking of CC. The information supports life cycle SE activities, in addition to being a basis for program protection planning. The information contained in the authoritative database (e.g., PEO CC database) should be structured and related to allow for easy access and for attribute-specific query. Note that the ASDB is an authoritative database for CPI, but does not apply to CCs.

8.0. References

Guidance

- AFPAM 63-113, Program Protection Planning for Life Cycle Management, 17 October 2013.
- Defense Acquisition Guidebook (DAG), 30 September 2019[35]
- Department of Defense Anti-Tamper Desk Reference, Second Edition, April 2017.
- (U) DoD Anti-Tamper (AT) Technical Implementation Guide (TIG) (Document is classified SECRET), CH-1, 27 December 2018.
- DoDM S-5230.28, (U) Low Observable (LO) and Counter Low Observable (CLO) Programs Manual (SECRET), 28 December 2016.
- DASD, "Systems Engineering, Program Protection Plan Outline & Guidance", V1.1, February 2014.

Legal

- FR, Vol. 86, No. 93, Executive Order 14028, 12 May 2021.
- ITAR 22 CFR 120-130. International Traffic in Arms Regulation (ITAR).[36]
  The Department of State is responsible for the export and temporary import of defense articles and services governed by 22 U.S.C. 2778 of the Arms Export Control Act (AECA) and Executive Order 13637. The ITAR implements the AECA.
- 32 CFR 236.4, "Cyber Incident Reporting Procedures", 1 July 2020.

Standards

- FIPS 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," Aug 2013.
- CNSSI No. 4009, 6 April 2015.
- ISO/IEC/IEEE 15288:2015, "Systems and Software Engineering – Systems Lifecycle Processes", May 2015...

[35] https://www.dau.mil/tools/dag

[36] https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987

Policy

- AFPD 63-1/20-1, Integrated Life Cycle Management, 7 August 2018.
- Air Force Instruction 63-101/20-101, Integrated Lifecycle Management, 30 June 2020.
- DoDI 5200.47E, “Anti-Tamper”, CH-3, 22 December 2020.
- DoDI 4140.67, DOD Counterfeit Prevention Policy, CH-3, 6 March 2020.
- DoDI 5000.02, “Operation of the Adaptive Acquisition Framework”, 23 January 2020.
- DoDI 5200.39, Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E), CH-3, 1 October 2020.
- DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”, CH-3, 15 October 2018.

Reports

- Industrial Base Assessments – the U.S. Department of Commerce, The Office of Technology Evaluation (OTE) utilizes its unique designated authority to conduct surveys and assessments of defense-related technologies, and to monitor economic and trade issues vital to the U.S. industrial base as specified in congressional mandates and Executive Orders. OTE conducts primary research and analysis of critical technologies and industrial capabilities of key defense-related sectors. The office uses industry-specific surveys to obtain essential employment, financial, production, research and development, export control, and other data – information unavailable from any other source. **https://www.bis.doc.gov/index.php/other-areas/office-of-technology-evaluation-ote/industrial-base-assessments**

- U.S. Department of Commerce’s International Trade Administration implemented the Export Control Reform Initiative (ECR Initiative), which fundamentally reformed the U.S. export control system. The ECR Initiative, which is not related to the President’s National Export Initiative, is designed to enhance U.S. national security and strengthen the United States’ ability to counter threats such as the proliferation of weapons of mass destruction. **https://www.trade.gov/export-solutions**

Templates

- “CPI Assessment and Identification Guide (CAIG)”, V1.0,”, NDIA, 2 Aug 2019 (FOUO) **https://at.dod.mil/**
- “CPI/LO/CLO Workbook Template 1.0 , Classified HPG and 5230 Tabs,” 2 August 2019 (SECRET): request through **https://at.dod.mil/**

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

APPENDIX C

FUNCTIONAL THREAD ANALYSIS

Version 4.0

26 July 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Secretary of the Air Force, Public Affairs (SAF/PA) Case #: 2021-0424. Requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

Table of Contents

Table of Tables

Table of Figures

FOREWORD

“USAF Systems Security Engineering Acquisition Guidebook” introduces the Functional Thread Analysis (FTA) workflow process and its identification of a system’s cyber APVs for the subsequent Attack Path Analysis (APA)/Attack Path Exercise processes to the reader.

Record of Changes

Version	Effective	Summary
4.0	26 July 2021	Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	Addition of Space Systems into SSE requirements assessment process.
3.0.1	29 Jan 2021	No changes to content, just updated revision numbers to correspond with body of the main document.

1.0. SCOPE.

The scope of Appendix C is to provide guidance on how to functionally decompose a system from its highest-level User requirements to their lowest possible component levels, perform a Criticality Analysis that identifies system vulnerabilities locating their associated EAPs, and create APVs for their follow-on Attack Path Analysis (APA)/Attack Path Exercise (APE) (see Appendix D).

2.0. BACKGROUND.

The Functional Thread Analysis (FTA) begins by completing a functional decomposition of the system mission capabilities identified in the HPT-defined User requirement documents (e.g., Information Security Initial Capabilities Document [IS-ICD], Capabilities Development Document [IS-CDD]). The capabilities are further decomposed and allocated to the mission(s) required for the system capabilities.

The SSWG works closely with the High Performance Team (HPT) to prioritize missions ([37]) using the precepts and tenants of the USD (R&E) Mission Engineering (ME) Guide. Digital engineering principles should be used when conducting ME as they can help promote consistency in the ME process through the effective use and reuse of curated data and models along with identification and utilization of digital tools throughout ME analyses. Digital engineering is an essential foundational element of ME that allows for sustainment of Mission Threads (MTs) and architectures, integrated analytical capabilities, common mission representations, and an extensible set of tools.

2.1. MISSIONS FOR SPACE AND WEAPON SYSTEMS.

Space and Weapon System missions are derived from the Universal Joint Task List (UJTL) into Joint Mission Essential Task List (JMETL).

Along with the Joint Mission Essential Task List (JMETL), the service-specific Mission Essential Task List (METL) are used as the basis for the Air Force Doctrine Publication (AFDP)-series and the Air Force Task List (AFTL) as discussed by the AFDP 1, "Air Force Capstone Doctrine, 10 March 2021.[38]

The AFDP 2-0, 3-series and 4-series provide specific warfare operations by generic USAF warfare communities, but not specific to a space and weapon system Type. Model and Series (TMS) family.

The AFTL and the UJTL along with the space and weapon system ICD, CDD, CONOPS, and ROC/POE and their JCIDS delineated KPPs, METs, Conditions and Standards are used to develop the Mission-based Critical Operational Issues (COI) for the particular space and weapon system family or TMS under Mission Engineering (ME) analysis.

Critical Operational Issues (COI) are the operational effectiveness and operational suitability issues (not parameters, objectives, or thresholds) that must be examined to evaluate/assess the system's capability to perform its mission. Not all operational issues are critical. COIs must be relevant to the required

[37] **Appendix A: USAF SSE Acquisition Guidebook, Section 1.1.2**

[38] **https://www.doctrine.af.mil/**

capabilities for a system to be operationally effective and suitable and represent a significant risk if not satisfactorily resolved.

COIs must be examined and related to Measures of Effectiveness (MOE) and Measures of Suitability (MOS), and are included in the Test and Evaluation Master Plan (TEMP).

A COI is normally phrased as a question that must be answered in the affirmative to properly evaluate operational effectiveness. The following are four examples of COI statements in the TEMP:

- Will the platform/system (or subsystem/equipment) detect the threat in a combat environment at the adequate range to allow a successful mission?

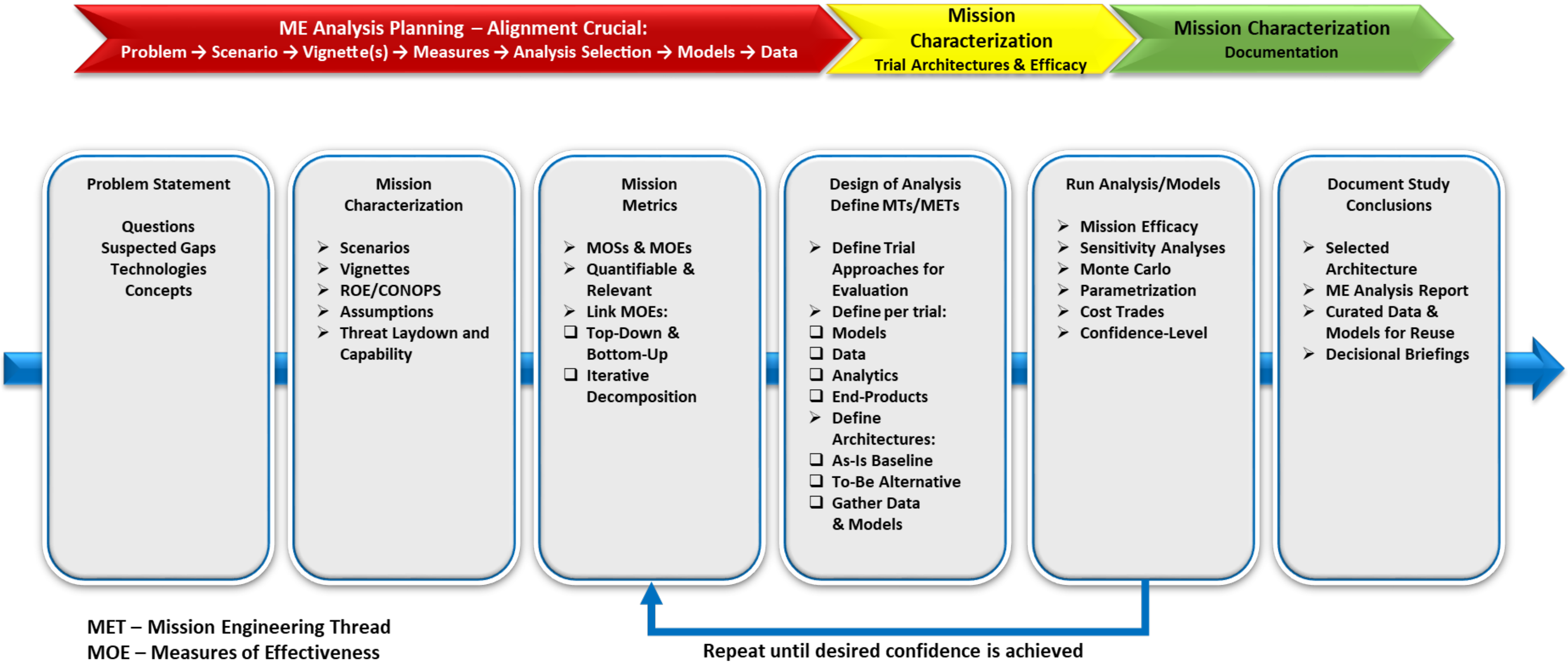
- Will the system be safe to operate in a combat environment?

- Can the platform/system (or subsystem/equipment) accomplish its critical missions?

- Is the platform/system (or subsystem/equipment) ready for Joint and, if applicable, Combined operations?

Missions can further be decomposed into the functions required to execute the mission using the ME process. Key factors with the SSWG HPT to consider are:

- What is the primary mission? What are the secondary/tertiary missions (if applicable)?
- What are its boundaries and how must it interact with other missions?
- What are its performance measures?
- What are the mission capability gaps?
- How can new capabilities change the way we fight?
- What do changes in capabilities or systems mean to missions and architecture?
- What is the sensitivity of the mission performance to the performance of the constituent technology, products and capabilities?
- How do new capabilities best integrate with or replace legacy systems?
- How do we optimize that balance to provide the most lethal and affordable integrated capabilities for any particular mission?



MET – Mission Engineering Thread
MOE – Measures of Effectiveness
MOS – Measures of Success
MT – Mission Thread
ROE – Rules of Engagement

Figure C-1 Mission Engineering (ME) Workflow Process Diagram

Figure C-1 illustrates the ME process as a part of the HPT's analyses in characterizing the weapon system's intended missions and their capability profiles within the intended operating environment.

The major products from ME analysis include:

- Documented results in the form of analytical reports, curated data and models for continued reuse and further analysis
- Visualizations and briefings to inform leadership on key decisions and;
- Government Reference Architectures (GRA) (in the form of diagrammed depictions of missions and interactions amongst elements associated with missions and capabilities)

While conducting the functional decomposition, it is necessary to identify functions that are mission critical, as well as, safety critical. DoDI 5200.44 defines Mission Critical Functions (MCFs) as, "… any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed." MIL-STD-882 defines Safety Critical Functions (SCFs) as, "… a function whose failure to operate or incorrect operation will directly result in a mishap of either Catastrophic or Critical severity."

The identification of MCFs and SCFs enable the program to concentrate on where and Information on how to implement Cybersecurity and Cyber Resiliency requirements. Functions can then be further allocated to the systems/subsystems/Line-Replaceable Units (LRUs)/components (e.g., hardware and software) required to execute these functions.

A program may contain Critical Program Information (CPI), which can be associated with particular functions. DoDI 5200.39 defines CPI as, "*United States (U.S.) capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.*"

Upon documenting systems, subsystems, and components, **Appendix B: USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components (CC) Identification**, can be used to identify CCs and CPI. CCs may or may not be an LRU. Depending on the program, an LRU could be also referred to as Weapon Replaceable Assembly (WRA), composed of Shop Replaceable Units (SRU)/Shop Replaceable Assemblies (SRA). The concept is to decompose the system all the way down to the component level. The success of these efforts depends heavily on the maturity of the system.

A graphical representation of this decomposition is in Figure C-2.

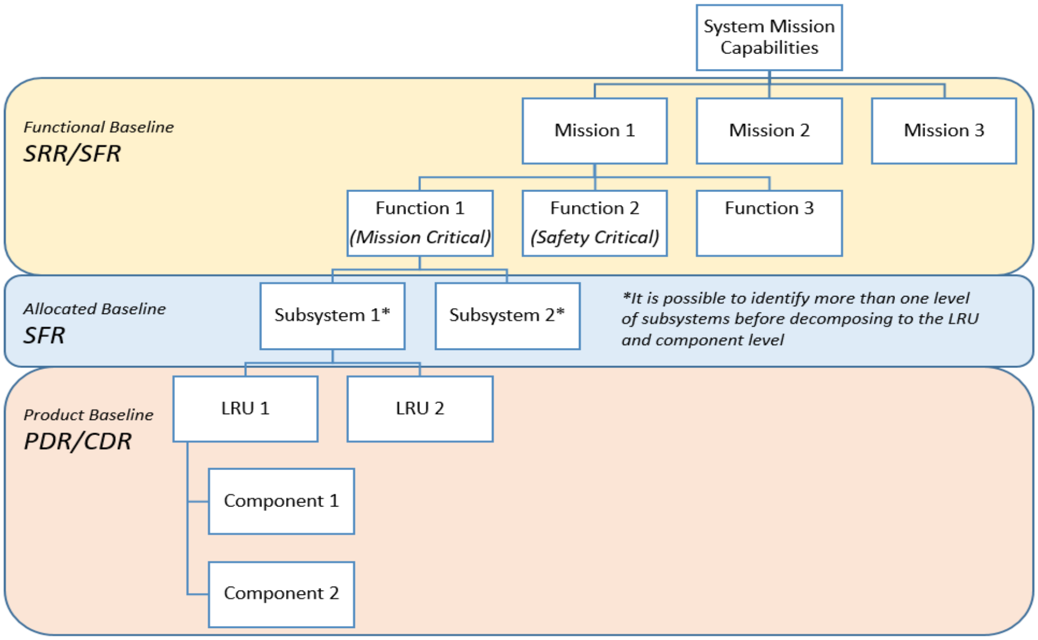

System Mission Capabilities
Functional Baseline
SRR/SFR
Mission 1
Mission 2
Mission 3
Function 1 (Mission Critical)
Function 2 (Safety Critical)
Function 3
Allocated Baseline
SFR
Subsystem 1*
Subsystem 2*
*It is possible to identify more than one level of subsystems before decomposing to the LRU and component level
Product Baseline
PDR/CDR
LRU 1
LRU 2
Component 1
Component 2

Figure C-2 Functional Decomposition Example

In addition to the functional decomposition, the FTA identifies vulnerabilities within the system and pairs those vulnerabilities with subsystems/components. The subsystems/components that are identified as vulnerable are further analyzed to determine if they could be Entry Access Points (EAPs). An EAP is defined as ”Possible points of entry into a system that could be used to alter the system software and/or hardware (including disabling or damaging), to cause the system to behave differently as it is running, or to extract information from the system. These are typically non-logic bearing units such as data ports, card readers, antennas, CD-ROM drive, etc.[39]

After the functional decomposition, the vulnerability analysis, and EAP identification, the SSWG will develop Attack Path Vignettes (APVs) that will be used to conduct the Attack Path Analysis (APA)/Attack Path Exercise (APE)[40]; see Appendix D. The vignettes utilize the previously EAP identification and functional decomposition to map out possible cyber-events that exploit potential vulnerabilities between the attack surface and the target components.

The FTA is an iterative process that should be updated in concert with a program’s Systems Engineering Technical Reviews (SETRs). The fidelity of this analysis will increase as the program matures through its Adaptive Acquisition Framework (AAF) lifecycle. The earliest that the FTA occurs is within the activities to characterize the system as in WBS 1.2 (Figure C-2). Further details regarding the expected fidelity of the FTA are located in the subsequent sections of the WBS. Since cyber related events are a continually evolving and growing operational risk to all space and weapon systems, it is critical to factor in active

[39] “Avionics Cyber Vulnerability Assessment And Mitigation Manual”, AFRL, March 2014.
[40] United States Air Force, “Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook”, Version 2.0, 1 April 2020.

threat data and operational experience that may impact future design changes, upgrades, mitigations and/or the development of new Tactics, Techniques, and Procedures (TTP). The FTA should be informed by the information and data provided from CDRL 15 (Contractor's FTA DID); see **Appendix A: USAF SSE Acquisition Guidebook, Attachment 2**.

Ultimately, by conducting the FTA (Appendix C) and APA (Appendix D) during the execution of the SSE Cyber Workflow Process, programs will discover cyber-related and programmatic risks. Risk assessments should be used by the Program Manager to determine where, when and how risk mitigations can be applied to the space and weapon system's design that addresses operations in CONOPS-specified operational environments. Mitigating these risks should be done through allocation or implementation of the SSE requirements located in **Appendix A: USAF SSE Acquisition Guidebook, Attachment 1, an Excel workbook**.

3.0. FUNCTIONAL THREAD ANALYSIS

The following sections address the functional decomposition and the vulnerability analysis.

3.1. FUNCTIONAL DECOMPOSITION

The first part of a FTA is decomposing the system, ultimately down to the component level. The subsections below outline the function decomposition's level of fidelity expected at the given Systems Engineering Technical Reviews (SETRs). It is important to note that the decomposition is done "in support of" the SETRs, therefore it is imperative that the SSWG does not wait until the SETR is ready to occur, rather the work should be done in the months preceding the review. The following SETRs are addressed:

- System Requirements Review (SRR)
- System Functional Review (SFR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)

3.1.1. FUNCTIONAL DECOMPOSITION & SYSTEM REQUIREMENTS REVIEW (SRR).

By SRR, CSAs should be allocated to system missions. Those missions need to be decomposed into the MCFs, SCFs, and Functions associated with CPI (F-CPI), if F-CPI are known, that are responsible for executing that mission. This is accomplished by reviewing the following documents:

- User Requirements (e.g., IS-ICD, IS-CDD, FRD, UON), to include the applicability of the Cyber Survivability Attributes (CSA) as seen in Table C-1 as an example. If the information in Table C-1 is not provided in the User Requirements documents, then the Program Office will need to provide this data.
- System Requirements Document (SRD) or System/Subsystem Specification (SSS) to include the applicable system level requirements from: **Appendix A: USAF SSE Acquisition Guidebook, Attachment 1 Excel file; and/or those specified by the SMC SWG**
- System Characterization.

- Concept system level architecture to include the following DoD Architecture Framework viewpoints:
    - AV-1: Overview and Summary Information
    - OV-1: High-Level Operational Concept Graphic
    - OV-2: Operational Resource Flow Description
    - OV-4: Organizational Relationships Chart
    - OV-5b: Operational Activity Model
    - OV-5a: Operational Activity Decomposition Tree

NOTE: Update the architecture viewpoints as applicable.

After reviewing the documentation, the SSWG should document their findings in a table similar to the one seen in Table C-1.

Table C-1 Example CSA Applicability to Missions

	CSA 1	CSA 2	CSA 3	CSA 4	CSA 5	CSA 6	CSA 7	CSA 8	CSA 9	CSA 10	Criticality / Consequence
Mission 1											
Mission 2											
Mission 3											

The size of Table C-1 is dependent upon the number of Missions. Criticality/Consequence should be determined as per DoDI 5200.44 and CNSSI No. 1253 (i.e., impact levels for Confidentiality, Integrity, or Availability [CIA]), and the DAG, Chapter 9, Table 3 (i.e., Criticality Levels I through IV corresponding with the consequence of their failures within the space and weapon system's ability to perform its mission).

After identifying the missions and associated CSAs, the missions need to be decomposed into the MCF, SCFs, and Functions associated with CPI that are responsible for executing that mission, as stated previously. A table similar to Table C-2 is populated to map the missions to their corresponding MCFs, SCFs, and Functions associated with CPI.

Table C-2 Missions Responsible for MCFs, SCFs, and functions associated with CPI

	Mission 1	Mission 2	Mission 3	Criticality / Consequence
MCF 1				
MCF 2				
SCF 1				
SCF 2				
CPI 1				
CPI 2				

The dimensions of Table C-2 is dependent upon the number of MCFs, SCFs, and CPI functions identified, as well as, the number of missions identified. Criticality/Consequence should be determined as per DoDI 5200.44 and CNSSI No. 1253 CIAs, and DAG, Chapter 9, Table 3 (i.e., Criticality Levels I through IV corresponding with the consequence of their failures within the space and weapon system's ability to perform its mission).

A table similar to Table C-3 is populated to identify and document how the MCFs, SCFs, and CPI functions identified interface with one another.

Table C-3 MCFs/SCFs/CPI Functions & Interfaces (Internal and External)

	MCF 1	MCF 2	SCF 1	SCF 2	CPI 1	CPI 2
MCF 1						
MCF 2						
SCF 1						
SCF 2						
CPI 1						
CPI 2						

Table C-3 should be populated with the Interface Control Document identifier(s) (i.e. the document identification number) that details the interfaces, where possible.

3.1.2. INFORMATION TO DOCUMENT IN THE FTA REPORT.

- The system's concept of operation to include the missions and functions that will achieve the concept of operation.
- MCFs, SCFs, and Functions associated with CPI.
- Mission integrated CSAs (Table C-1).
- The mission including the MCFs, SCFs, and Functions associated with CPI (Table C-2).
- System attributes such as boundaries, adjacency/dependency; internal/external to system connections; type/functionality; redundancy, etc. (Table C-3).
- All known data sources and data receivers.
- Updated Risk Assessment per Work Breakdown Structure (WBS) for the USAF Systems Security Engineering (SSE) Cyber Guidebook (SSECG) Process, step 4.4 Risk Assessment.

3.1.3. FUNCTIONAL DECOMPOSITION & SYSTEM FUNCTIONAL REVIEW (SFR).

The functional decomposition from SRR is updated to reflect the additional information known at SFR. The following documents will assist in the update to the functional decomposition:

- SRR functional decomposition (**NOTE:** this should be documented in an FTA report)
- User Requirements (IS-ICD, IS-CDD, FRD, UON)
- System Requirements Document (SRD)
- System and subsystem specifications, including the applicable system and subsystem level requirements from:

  Appendix A: SSE Acquisition Guidebook, Attachment 1 Excel file
- Criticality Analysis
- Completed system level architecture to include the following DoD Architecture Frameworks:
  - AV-1: Overview and Summary Information
  - OV-1: High-Level Operational Concept Graphic
  - OV-2: Operational Resource Flow Description
  - OV-4: Organizational Relationships Chart
  - OV-5b: Operational Activity Model
  - OV-5a: Operational Activity Decomposition Tree
  - SV-4: Systems Functionality Description
  - SV-5: Operational Activity to System Function Traceability Matrix
  - SV-6: Systems Data Exchange Matrix

  NOTE: Update the architecture viewpoints, as necessary.

3.1.4. INFORMATION TO DOCUMENT IN THE FTA REPORT.

- MCFs, SCFs, and Functions associated with CPI mapped to the subsystems that are responsible for those functions (Table C-4)
- The manufacturer (mfr.) is responsible for each subsystem (Table C-4).
  NOTE: If specific subsystem components are known at this time, requests for DIA TAC reports should be submitted.
- Updates (i.e., additional details) to the system attributes such as boundaries, adjacency/dependency; internal/external to system connections; type/functionality; redundancy, etc. (Table C-5)
- Include known service type, linkages and type, directionality, digital/analog, etc.
- All known data sources and data receivers.
- Updated Risk Assessment as per the WBS for the USAF Weapon System PP and SSE Workflow Process, step 4.4, “Risk Assessment”.

After completing the documentation review, tables similar to Table C-4 and C-5 will be populated. This decomposition identifies the subsystems that are responsible for completing the missions and the functions that support the subsystems. Additionally, the interfaces between the subsystems will be identified, which will help inform the attack path analysis.

Table C-4 Systems/Subsystems Responsible for MCFs, SCFs, & CPI functions

	Mission 1 *(mfr.)*			Mission 2 *(mfr.)*		Mission 3 *(mfr.)*	Criticality / Consequence
	Subsystem a *(mfr.)*	Subsystem b *(mfr.)*	Subsystem c *(mfr.)*	Subsystem b *(mfr.)*	Subsystem d *(mfr.)*	Subsystem e (mfr.)	
MCF 1							
MCF 2							
SCF 1							
SCF 2							
CPI 1							
CPI 2							

The dimensions of Table C-4 is dependent upon the number of MCFs, SCFs, and CPI Functions identified, as well as, the number of subsystems identified. Criticality/Consequence should be determined as per DoDI 5200.44 and CNSSI No. 1253 CIAs, and DAG, Chapter 9, Table 3 (i.e. Criticality Levels I through IV corresponding with the consequence of their failure of the system’s ability to perform its mission).

Table C-5 Subsystem to Subsystem Interfaces (Internal and External)

	Subsystem a	Subsystem b	Subsystem c	Subsystem d	Subsystem e
Subsystem a	▨				
Subsystem b		▨			
Subsystem c			▨		
Subsystem d				▨	
Subsystem e					▨

Table C-5 should be populated with the Interface Control Document identifier(s) detailing the subsystem-to-subsystem interfaces.

3.1.5. FUNCTIONAL DECOMPOSITION & PDR AND CDR

The SFR's functional decomposition is updated to include the detailed system design information for PDR. Subsequently, the PDR functional decomposition is updated for CDR. Documents reviewed and information required in the PDR and CDR functional decomposition reports should be considered initial and final, respectively. The following documents will assist in the update to the functional decomposition:

- SFR functional decomposition
  - User Requirements (IS-ICD, IS-CDD, FRD, UON)
  - System Requirements Document (SRD)
  - System, subsystem, LRUs/component specifications, to include the applicable system and lower level requirements from: **Appendix A: USAF SSE Acquisition Guidebook, Attachment 1 Excel file**
  - **Criticality Analysis (CA)** – heavily dependent on the prioritization of system functions.
  - Information Support Plan (ISP)
  - Completed system level architecture including the following DoD Architecture viewpoints:
    - AV-1: Overview and Summary Information
    - OV-1: High-Level Operational Concept Graphic
    - OV-2: Operational Resource Flow Description
    - OV-4: Organizational Relationships Chart
    - OV-5b: Operational Activity Model
    - OV-5a: Operational Activity Decomposition Tree

- SV-4: Systems Functionality Description
- SV-5: Operational Activity to System Function Traceability Matrix
- SV-6: Systems Data Exchange Matrix

  NOTE: Update the architecture viewpoints, as needed.

Tables C-6 and C-7 will be populated in support of PDR, and Tables C-8 and C-9 will be populated by CDR.

Table C-6 Systems/Subsystems, & LRUs with MCFs, SCFs, & CPI functions

	Mission 1							Mission 2				Mission 3		Criticality / Consequence
	Subsystem a *(mfr.)*			Subsystem b *(mfr.)*		Subsystem c *(mfr.)*		Subsystem b *(mfr.)*		Subsystem d *(mfr.)*		Subsystem e *(mfr.)*		
	LRU 1 *(mfr.)*	LRU 2 *(mfr.)*	LRU 3 *(mfr.)*	LRU 2 *(mfr.)*	LRU 4 *(mfr.)*	LRU 3 *(mfr.)*	LRU 5 *(mfr.)*	LRU 2 *(mfr.)*	LRU 4 *(mfr.)*	LRU 6 *(mfr.)*	LRU 7 *(mfr.)*	LRU 4 *(mfr.)*	LRU 7 *(mfr.)*	
MCF 1														
MCF 2														
SCF 1														
SCF 2														
CPI 1														
CPI 2														

The size of Table C-6 is dependent upon the number of MCFs, SCFs, and CPI Functions identified, as well as, the number of LRUs identified.

Criticality/Consequence should be determined in accordance with DoDI 5200.44 and CNSSI No. 1253 CIAs, and DAG, Chapter 9, Table 3 (i.e. Criticality Levels I through IV corresponding with the consequence of their failure of the system's ability to perform its mission).

NOTE: It is understood that LRU is a hardware-centric term; but also applicable to a Logic-Bearing Unit or Software Module.

Table C-7 LRUs to LRUs Interfaces/Adapters (Internal and External)

	LRU 1	LRU 2	LRU 3	LRU 4	LRU 5	LRU 6	LRU 7
LRU 1							
LRU 2							
LRU 3							
LRU 4							
LRU 5							
LRU 6							
LRU 7							

Table C-7 should be populated with the IS-ICD identifier(s) that details the LRU to LRU interfaces.

NOTE: It is understood that LRU is a hardware-centric term; but also applicable to a Logic Bearing Unit or Software Module.

Table C-8 Systems/Subsystems, LRUs, & Components with MCFs, SCFs, & CPI

	Mission 1															Mission 2										Mission 3					Criticality / Consequence
	Subsystem a *(mfr.)*							Subsystem b *(mfr.)*					Subsystem c *(mfr.)*			Subsystem b *(mfr.)*					Subsystem d *(mfr.)*					Subsystem e *(mfr.)*					
	LRU 1 *(mfr.)*			LRU 2 *(mfr.)*		LRU 3 *(mfr.)*		LRU 2 *(mfr.)*		LRU 4 *(mfr.)*			LRU 3 *(mfr.)*		LRU 5 *(mfr.)*	LRU 2 *(mfr.)*		LRU 4 *(mfr.)*			LRU 6 *(mfr.)*			LRU 7 *(mfr.)*		LRU 4 *(mfr.)*			LRU 7 *(mfr.)*		
Component (mfr.)*	1	2	3	4	5	6	7	4	5	8	3	9	6	7	10	4	5	8	3	9	7	2	1	9	3	8	3	9	9	3	
MCF 1																															
MCF 2																															
SCF 1																															
SCF 2																															
CPI 1																															
CPI 2																															

The manufacturer should be identified for each component

The dimensions of Table C-8 is dependent upon the number of MCFs, SCFs, and CPI Functions identified, as well as, the number of components identified. Criticality/Consequence should be determined in accordance with DoDI 5200.44 and CNSSI No. 1253 CIAs and the DAG, Chapter 9, Table 3 (i.e. Criticality Levels I through IV corresponding with the consequence of their failure of the system's ability to perform its mission).

NOTE: It is understood that LRU is a hardware-centric term; but also applicable to a Logic-Bearing Unit or Software Module.

Table C-9 Component Unique Interfaces/Adapters (Internal and External)

	Component 1	Component 2	Component 3	Component 4	Component 5	Component 6	Component 7	Component 8	Component 9	Component 10
Component 1										
Component 2										
Component 3										
Component 4										
Component 5										
Component 6										
Component 7										
Component 8										
Component 9										
Component 10										

Table C-9 should be populated with the IS-ICD identifier(s) that details the component to component interfaces.

3.1.6. INFORMATION TO DOCUMENT IN THE FTA REPORT.

- Complete identification of LRUs and components responsible for the MCFs, SCFs, and functions associated with CPI (Tables C-6 and C-8)

  NOTE: LRU is a hardware-centric term used for a Logic-Bearing Unit or Software Module.

- The manufacturer (mfr.) responsible for each LRU and component (Tables C-6 and C-8).

  NOTE: Once manufacturers are known, DIA TACs should be submitted.

- LRUs mapped to the LRUs (Table C-7) and components mapped to the components (Table C-9)
- All boundaries, interfaces/adapters identified, Entry Access Point (EAP)s, functions, ports and protocols, configuration management, etc.
- All known data sources and data receivers.
- Updated Risk Assessment as per the WBS for the USAF Weapon System PP and SSE Workflow Process, step 4.4, "Risk Assessment".

3.1.7. FUNCTIONAL DECOMPOSITION BEYOND CDR.

The functional decomposition is an ongoing assessment post-CDR and throughout the space and weapon system's operational deployment, where the operational assessments/re-assessments will re-occur. These include ensuring sustainment, monitoring of maintenance, supply chain, upgrades, etc. are fully addressed and implemented. Further, updates to the functional decomposition are based on threats, configuration management and the use data, etc. The information developed during the functional decomposition will inform the FTA, APA and risk assessments for the life of the program.

4.0. VULNERABILITY ANALYSIS

The purpose if the vulnerability analysis is to identify and analysis any vulnerability in the system. A vulnerability is defined as "weakness in system, system security procedures, internal controls, or implementation that could be exploited by a threat source (Ref. CNSSI No. 4009)." It is impossible to identify all potential vulnerabilities for a given component where a potential vulnerability is one that simply has not yet been verified. Therefore, this portion of the analysis is designed to identify potential vulnerabilities associated with the system components and to generate discussion towards design considerations and to eventually inform test strategy.

The analysis should consider inherited vulnerabilities from required system of system connections, including access points and attack paths that can be exploited to defeat a system's mission objectives or significantly degrade its performance (including exfiltration of data that can be used to negatively impact mission effectiveness of the targeted system or other mission systems). All aspects must be considered to include the development, production, test, and operational environments; this includes both industry and Government locations.

Using what is known about the system, brainstorm potential vulnerabilities stemming from attack possibilities as related to each EAP, CPI, and critical component. Document this analysis and any well-known or previously established vulnerabilities within the FTA report. The FTA reports results are critical to the implementation of the Mission-Based Cybersecurity Risk Assessment (FOUO) or its variance in the form of the Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook.

However, to achieve Mission Focused Cyber Hardening (MFCH) for Space and Weapon systems, one must apply standards, processes, and procedures across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) spectrum to achieve Operational Resilience through Cyber Survivability such that space and weapons systems, supporting assets, and infrastructure can execute defense critical missions throughout their life cycle in a cyber-contested environment.

Space systems are unique in their design and operational environment where their vulnerabilities, especially when regards to hardening of components and their associated failure modes and resultant effects could directly impact the system functionality and Operational Resiliency. Appendix D should be applied along with SMC-S-014 as it meets the verification and validation needs of the particular space system under design or modification.

4.1. ENTRY ACCESS POINT (EAP) IDENTIFICATION

Entry Access Points are identified by reviewing the functional decomposition (Section 3.1), system architectures, and vulnerability analysis (Section 5.0).

Due to system complexity, it is often difficult to identify all of the relevant data required to perform the identification. To assist, the Wheel of Access (WoA) tool is an organizational construct developed by the AFRL to help identify information exchanges and their respective EAPs. While each type of system has its own WoA model, they all provide a means to systematically review a system and identify data flows into or out of a system. Figure C-3 and C-4 illustrate two versions of the WoA model: the basic WoA model for a space and weapon system and an enhanced version referred to as the Platform Susceptibility Oriented WoA model. The Platform Susceptibility Oriented WoA model builds upon the traditional WoA, associating potential attack vectors associated with each respective wheel category and including potential “triggers” for cyber-attack vectors.

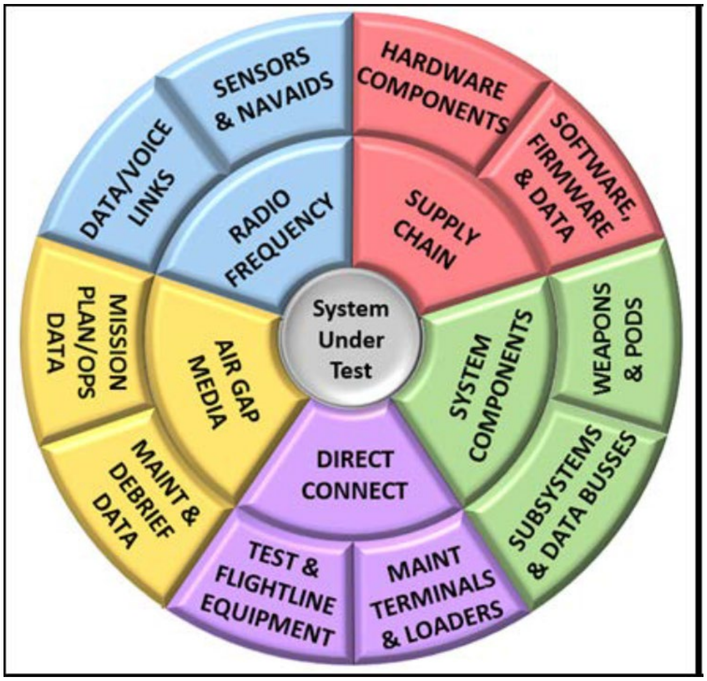
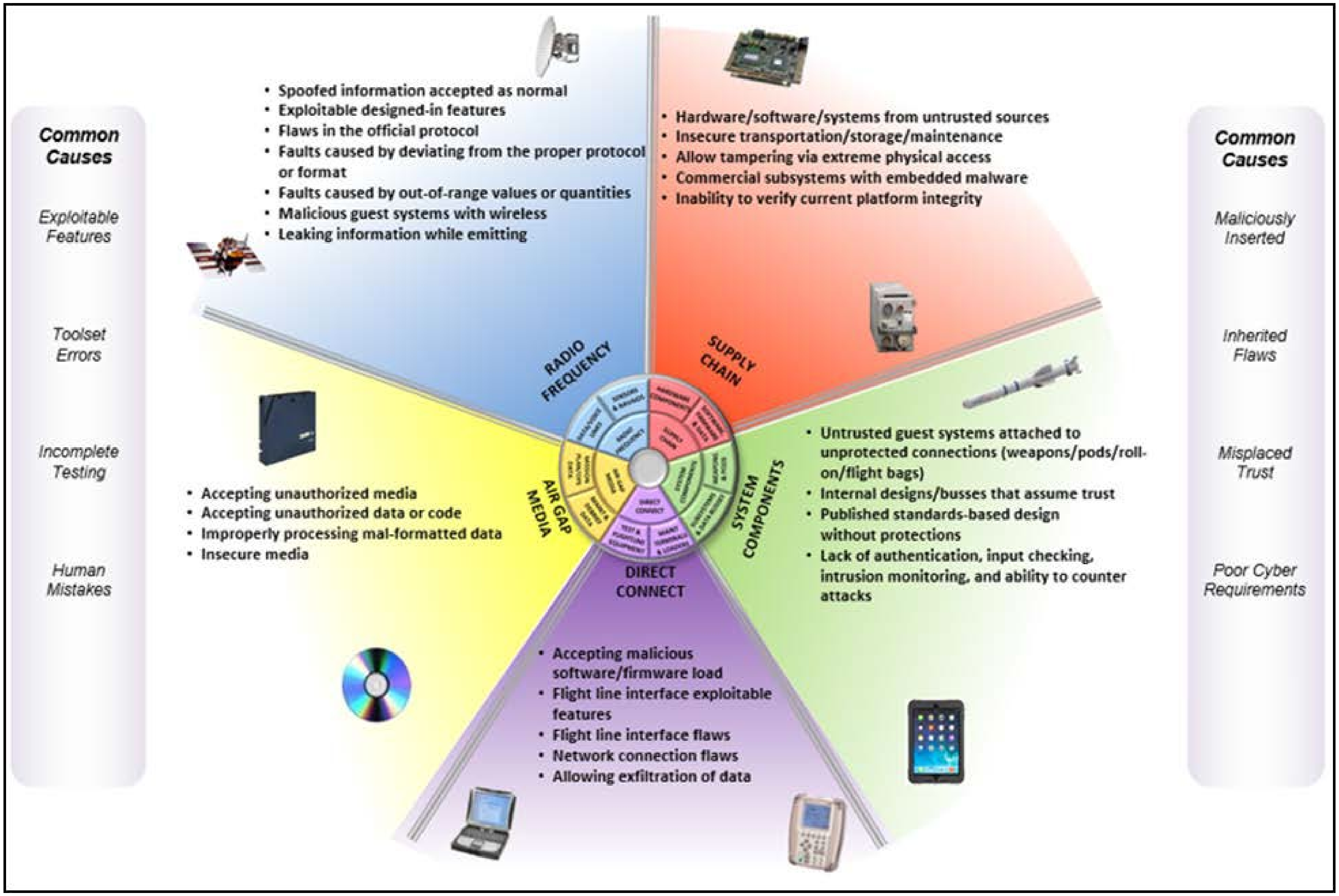


Figure C-3 Basic System WoA



- Spoofed information accepted as normal
- Exploitable designed-in features
- Flaws in the official protocol
- Faults caused by deviating from the proper protocol or format
- Faults caused by out-of-range values or quantities
- Malicious guest systems with wireless
- Leaking information while emitting

- Hardware/software/systems from untrusted sources
- Insecure transportation/storage/maintenance
- Allow tampering via extreme physical access
- Commercial subsystems with embedded malware
- Inability to verify current platform integrity

- Untrusted guest systems attached to unprotected connections (weapons/pods/roll-on/flight bags)
- Internal designs/busses that assume trust
- Published standards-based design without protections
- Lack of authentication, input checking, intrusion monitoring, and ability to counter attacks

- Accepting unauthorized media
- Accepting unauthorized data or code
- Improperly processing mal-formatted data
- Insecure media

- Accepting malicious software/firmware load
- Flight line interface exploitable features
- Flight line interface flaws
- Network connection flaws
- Allowing exfiltration of data

Figure C-4 Platform Susceptibility Oriented WoA

When utilized, the WoA model can help teams:

- Identify and categorize system EAPs and their corresponding interfacing systems both inside and outside the system boundary
- Analyze each EAP to identify potential vulnerabilities in:
    - Specification: protocols, capabilities, use modes
    - Architecture: information flows, byzantine failures, resource sharing
    - Implementation: hardware, software configuration
- Systematically categorize system interfaces
- Identify potential attack vectors and attack paths in the system's design
- Identify interfacing systems which might have vulnerabilities impacting the system
- Understand cyber relationships among system components and sub-systems
- Develop comprehensive and tailored Mission Based Cyber Risk Assessments (MBCRAs), Cooperative Vulnerability Identification (CVI), Adversarial Cyber Developmental Test and Evaluation (ACD), Cooperative Vulnerability and Penetration Assessment (CVPA), and Adversarial Assessment (AA)
- Evaluate design considerations and recommend Cyber Survivability requirements
- Identify potential test resource requirements (e.g., labs and agencies needed to test specific potential vulnerabilities and/or access categories)

Look at each section of the WoA to systematically identify and categorize all information exchanges through the system's cyber boundary. The EAP is where the external data flows pass through the cyber boundary such as with radio antennae, data card slots, and maintenance ports. Each EAP represents the beginning of a potential attack path into the system.

All analysis and results completed while identifying the EAPs, should be documented in the FTA report accordingly. The FTA report is critical to performing the APA discussed in Appendix D.

4.1.1. EAP CONSIDERATIONS FOR CPS[41][42]

CPS are not the typical product, system, SoS or application design in that they have significantly more interconnectivity internally and externally to other digital and analog, data and components.

Figure C-5 illustrates a CPS Conceptual model.

CPS involve sensing, computation and actuation systems that maybe directly, indirectly or isolated from other systems. When the CPS handling data flows from sensors for further computational purposes, and

[41] NIST Special Publication 1500-201, "Framework for Cyber-Physical Systems: Volume 1, Overview", v1.0, June 2017.

[42] NIST Special Publication 1500-202, "Framework for Cyber-Physical Systems: Volume 2, Working Group Reports", v1.0, June 2017.

This affects the control and actuation aspects of the CPS along with timing constraints; we are dealing in non-traditional IT Information Systems or Systems-of-Systems.

4.1.2. THINGS TO CONSIDER WHEN APPLYING THE WOA TO CPS ARE:

- **Bridging of Multiple Platforms**
  CPS operational capabilities maybe dependent on other systems across time and data domains. Therefore, data translation or conversion (e.g. timing stamps, latency, scales and accuracies) maybe required, posing an EAP in themselves.

- **The Open Nature of CPS**
  Interoperability with other CPS poses a unique challenge for cybersecurity and cyber resiliency (e.g. data links for sensor-to-remote CPWS fire control systems) risk mitigation.

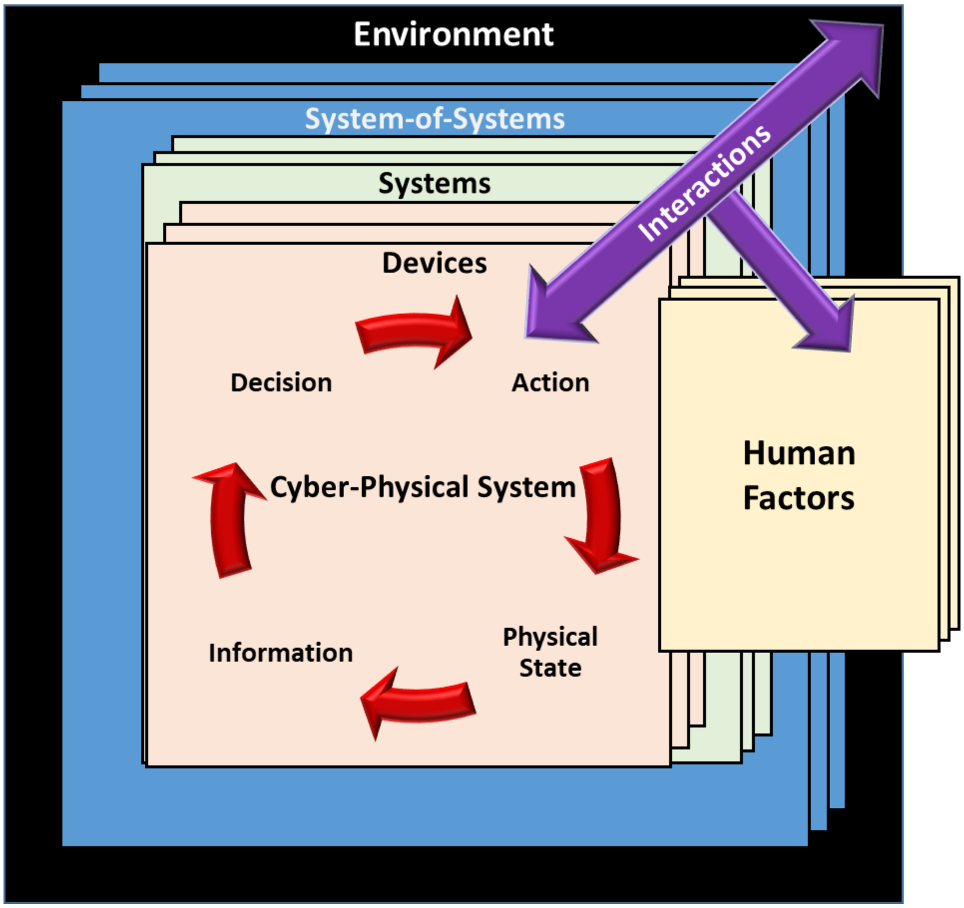


Figure C-5 CPS Conceptual Model

- **<u>Repurposed CPS</u>**
  Modifications to CPS affects not only their singular operational behavior, but also that of other interconnected CPS. (e.g., indirectly, these modified systems may affect internal power budgets causing other critical functioning systems to be at risk.)

- **<u>Cross-Domain CPS</u>**
  EAP for Cross-Domain systems and applications affect external systems.

- **<u>TSN Risks Heightened in CPS</u>**
  The required messaging, Certificate Authorities (CA), subscriptions and registries, to name a few potential trust associated risks, are often owned and managed by other systems, or the CPS does likewise own and manage such for external systems.

- **<u>Dynamic Components used in CPS</u>**
  Once a CPS is powered on and booted up, hardware or software components maybe modified as is the architecture causing a variation of EAP parameters that must be considered.

- **<u>CPS Complexity Issues</u>**
  Each SoS and component within a CPS have differences in their algorithms and computational complexities due to the computational and physical components of each SoS. The very differentiation in their computational ranges allows for EAP exploitation.

- **<u>CPS Communications Modes and Nodes</u>**
  The variation of interoperable CPS network connections (e.g., data links, internal networks) and in their protocols (i.e., legacy through object rich exchange) not only poses difficult EAP modeling and analyses, but affects the CPS energy budget, indirectly determining which CPS SoS may have to be turned on or off for a particular mission.

- **<u>CPS Control System and Sensing Loops</u>**
  CPS by the very nature in design and components have feedback loops within their architectures. Adding to this innate complexity as opposed to traditional IT Information System modeling are systems spanning static and adaptive controls, sensors and multi-modal sensors, and local, distributed, federated and centralized control system architectures, data fusion, and loosely or tightly coupled control and sensor systems. It is here where Cyber Resiliency elements can reduce or "Bake-In" solutions to these inherent design risks or their associated complex EAPs.

- **<u>CPS Environmental Associated EAPs</u>**
  All CPS measure and sense their operating environment along with their internally controlled environment for systems and human factors. A CPS component can behave as erratic as a human operator in the mission environment causing concern for the many modes of the components and human element (e.g. Helmet displays integrated with Instrument Landing Systems [ILS] at night, or targeting systems in high humidity weather) causing EAPs not specifically design inherent.

4.2. ATTACK PATH VIGNETTES

The Attack Path Vignettes (APVs) utilize the FTA to map out possible cyber-attack scenarios, which exploit potential vulnerabilities between the attack surface and the target components. The APVs summarize potential attack paths to the CPI/CC, vulnerabilities exploited along that path, actions taken by the aggressor, attack methodologies, attack goals, anticipated mission effects, and proposed test methodology. They provide a brief system description and identify assumptions, supporting intelligence information, and vignette risk and priority information. Because insufficient time and resources exist to develop APVs for all potential attack paths through the system, APVs will be generated which exploit potential vulnerabilities in high risk EAPs and their identified potential vulnerabilities along the attack path deemed most likely by the team throughout the system to the CPI/CC.

Table C-10 Documents to Review in Support of Decision Points

	MS-A	SRR	SFR	PDR	MS-B	CDR	Post CDR
Completed FTA	X	X	X	X	X	X	X
CONOPS/CONEMP	X	X	X	X	X	X	X
[Draft/Approved] Available system requirements documents (e.g., IS-CDD, SRD, CPD, FRD)	X	X	X	X	X	X	X
Interface Control Document		X	X	X	X	X	X
Specifications (System, Sub-System), LRU, H/W, S/W, component, etc. …			X	X	X	X	X
Interface Control Documents and Data Flows			X	X	X	X	X
Completed system level and Sub-System level architectures			X	X	X	X	X
OV-1: High-Level operational concept Graphic	X	X	X	X	X	X	X
OV-2: Operational Resource Flow Description			X	X	X	X	X
SV-4: Systems Functionality Description			X	X	X	X	X
SV-5: Operational Activity to System Function Traceability Matrix		X	X	X	X	X	X
SV-6: Systems Data Exchange Matrix		X	X	X	X	X	X

	MS-A	SRR	SFR	PDR	MS-B	CDR	Post CDR
Architecture functional models			X	X	X	X	X
Failure Modes Effects and Criticality Analysis (FMECA) (reference CDRL 19 in Appendix A: USAF SSE Acquisition Guidebook, Attachment 2)				X	X	X	X
Anti-Tamper Plan/ Reports				X	X	X	X
Program Protection Plan (PPP)			X	X	X	X	X
Program Protection Implementation Plan (PPIP)			X	X	X	X	X
Safety Criticality Analysis	X	X	X	X	X	X	X
Interface Control Document (IS-ICD)				X	X	X	X
Cyber Boundary Diagram(s)	X	X	X	X	X	X	X
Available Intelligence/Threat Information	X	X	X	X	X	X	X
Fault Tree Analysis				X	X	X	X
Security Classification Guide	X	X	X	X	X	X	X

These cyber-attack scenarios combine identified potential cyber vulnerabilities into operationally representative cyber-attack paths. The APV should identify attack path nodes, methodologies, anticipated mission impacts, risk ratings, and potential test methodologies/resources. Once the APVs are completed, they become the focus areas of the APE and Cyber T&E Strategy. They help shape requirements, design changes, mitigations, risk management, programmatic decisions, and operator and exploitation recovery procedures.

The information contained within the APVs become the foundation for Developmental and Operational Testing of articulating components and potential vulnerabilities during cooperative cyber test events, and the mission effects that the testers will attempt to achieve during adversarial cyber testing. This information will in turn feed the Cyber T&E Strategy, captured in the TEMP and summarized in the PPP under Cybersecurity Strategy.

Up to this point, the identified CPI and logic bearing CCs will become the initial set of cyber-attack targets. The more mature the system design is, the higher the design fidelity of the analysis will be. As the system's design fidelity increases during its acquisition lifecycle, the fidelity of the APVs will increase. Attack paths will be generated from the external attack source to components supporting Safety Critical Functions (SCFs), Mission Critical Functions (MCFs), or functions associated with CPI. The attack paths will change as the design of the system matures and as a deeper understanding of the system vulnerabilities is gained. To account for these design changes, the APA will be updated iteratively throughout program development. For a system modification program, early attack path analysis can leverage the knowledge of the existing system's architecture and known vulnerabilities before the details of the modification's components are known.

As determined from the FTA, at least one vignette for each high risk EAP is drafted and classified in accordance with the program's SCG. The previous analysis results are then used to identify potential vulnerabilities within the system that could be exploited, enabling an attacker to gain access to the system and its critical components or CPI. Further guidance for this process is located within this Guide's WBS, Table 2, "Conduct Vulnerability Analysis", Task Area 1.2.6.3. In addition, one should consider any additional System-of-Systems (SoS) and Cyber-Physical System (CPS) vulnerabilities that may present themselves due to their independent and interdependent interactions with other internal and/or external systems.

4.2.1. DEVELOP APVS.

Commence the development of the APVs, which outline how an adversary could access critical components or CPI, compromise data confidentiality, integrity, and/or availability, and the resulting mission impacts, using the **APV Template** "Attack Path Analysis Template", or updating previously generated Attack Path Vignettes, and referencing available system architecture information and FTA data. These attack vignettes should reflect threats from trusted insiders, adversarial nation states, and terrorist organizations. Taking into consideration adversary tactics and known/presumed adversary capabilities/tools, further develop attacks that the system may expect to experience in its specified operational environments. These actions will result in improved recommendations, increased test operational realism and system mission capability effectiveness.

4.2.2. CONSIDER INTELLIGENCE & COUNTER-INTELLIGENCE VARIABLES OF:

- What is/are the attack goal(s)? (e.g. data exfiltration, mission kill, etc…)
- What is/are the attack target(s)?
- What is/are the attack vector(s) to the system?
- What is/are the attack EAPs?
- What is/are the attack path(s) through the system from the EAP to the attack target(s)?
- What is/are the attack access point(s) sources?
- What is/are the mechanism(s) of attack? (e.g., transmitting unauthenticated messages)
- What is/are the data source(s)?
- What is/are the data receiver(s)?
- What are the potential degraded mission capabilities that could be the result of an adversary exploiting a known attack path?
- What is/are the potential impact(s) if the confidentiality of CPI or other data is compromised or system data is exfiltrated to an adversary?

4.2.3. USING THE APV TEMPLATE DETERMINE AND DOCUMENT:

NOTE: an example is provided for each vignette section in italics.

[Vignette Identification Number]: [Attack Name]
Provide a unique vignette identification number and name to be used for vignette tracking purposes. If possible, include the intended mission effect, attack vector mechanism, attack target, and entry access point used for the attack in the vignette name. [Attack] [EAP] to [Impact] [Mission].

- *Vignette 1: Inject malicious logic into Electrical Power Drive Unit (EDPU) via Personal Computer Memory Card International Association (PCMCIA) receptacle to prevent Air Drop.*

- Operational Mission

Using the CONOPS and CONEMP, identify the operational missions the cyber-attack captured in the Attack Path Vignette is intended to impact. When possible, include where in the mission sequence the attack is likely to occur and when the intended effect would likely be realized.

- *Air Drop (personnel and cargo).*

- **Attack Objective / Mission Effect**

Identify intended objective using key information: Intended Effect, Mission, Mission Critical Function, Critical Program Information, payload, attack type, impact. If possible, limit one mission effect within a given Vignette. If the Attack Path Vignette could impact multiple missions, create a new Attack Path Vignette for each mission effect so they can be assessed independently.

- *Degrade Air Drop mission by deceiving aircrew through altitude and airspeed algorithm corruption (driving loss of data integrity). Malicious logic is triggered by geo-fence while in area of operations below specified altitude with corrupted data (i.e., airspeed and altitude) being displayed at time of Air Drop. Compromised airspeed and altitude data results in air drop being aborted for being (falsely) out of parameters. Lack of equipment drop results in warfighter not receiving critical supplies. Ineffective personnel drop results in injury to personnel and/or troops landing in incorrect location.*

- **System Description**

Identify components that will likely be impacted during this attack (e.g., pivot point, pass through), data protocols, noteworthy weaknesses/protections, and describe the nodes, related system information, and potential vulnerability to be exploited (if known). While a full nodal analysis would identify all possible paths from the source to the target, identify the most likely path based upon available intelligence and/or inputs from subject matter experts.

- **PCMCIA**: *data storage device, no formatting required, produced by [Company V], connects to platform via PCMCIA receptacle.*
- **HUMS**: *logical component used to display and record platform Health and Usage data, produced by [Company W], contains PCMCIA receptacle for download and upload of related system data. PCMCIA inputs are RS-242, outputs are MIL-STD-1553.*
- ***MAU (Modular Acquisition Unit)***: *logical component, produced by [Company X], converts analog data to digital, routes airspeed and altitude data to EDPU via MIL-STD-1553.*
- **EDPU**: *logical component, produced by [Company Y], used to process platform data, contains drivers to process information for platform display, communicates via MIL STD 1553.*
- **Display**: *logical component, produced by [Company Z], provides graphical depiction of flight data for aircrew.*

- **Supporting Graphics**

Provide graphics and/or diagrams that support this vignette (e.g., system architecture diagrams) with the attack path clearly identified.

- **Assumptions**

Identify any required assumptions that must be realized in order to achieve this attack and/or the intended effect. Assumptions made during the Attack Path Vignette generation process may also drive the generation of a RFI so that an effort can be made to validate or invalidate the assumption at a future date. If a RFI has been generated, annotate the unique RFI number from the RFI Log so it can be tracked. Some assumptions may need to be validated or invalidated through follow-on testing:

- *Adversary has physical access to PCMCIA card either in supply chain or in garrison (RFI # 16).*
- *Corrupted PCMCIA card is introduced through the supply system or via an insider.*
- *Corrupted PCMCIA card will be transported to and inserted into to the platform.*
- *Logic-bearing components will propagate malicious logic through the system.*
- *Aircrew will make air drop decisions based on displayed digital airspeed and altitude, versus stand-by instrumentation.*

- **Intelligence**

Identify intelligence information that supports this attack and the intended effect.

- *Adversary has knowledge of system architecture/operation.*
- *Adversary has knowledge of PCMCIA formatting techniques.*
- *PCMCIA card is manufactured overseas by a non-trusted vendor.*
- *Evidence of PCMCIA firmware modification on another platform.*

- **Potential Attack Method**

Describe the attack vector from the external source to the EAP, the attack path from the EAP to the intended target(s) through pivot points, and actions taken during the attack. The generated cyber-attacks should be logically plausible based on the technical data provided, but not yet necessarily tested and proven to work. Include the potential vulnerabilities that would be exploited with each step of the attack. Identified potential vulnerabilities would be validated or updated through follow-on test:

- *Introduce a counterfeit PCMCIA (P/N 52500102) card containing malicious logic into the maintenance supply system.*
  - *Potential Vulnerability: PCMCIA Supply Chain compromise*
- *Maintenance personnel accept compromised PCMCIA card into inventory*
  - *a. Potential Vulnerability: No PCMCIA authenticity verification*
- *Maintenance personnel transport compromised PCMCIA card to the platform.*
- *Maintenance personnel insert compromised PCMCIA card into the HUMS PCMCIA receptacle (EAP).*
  - *a. Potential Vulnerability: HUMS trusted data verification (integrity)*
- *Upon application of platform power, HUMS transmits malicious logic from compromised PCMCIA card to HUMS (EDPU) (Attack Target).*
  - *a. Potential Vulnerability: HUMS trusted data verification (integrity)*
  - *b. Potential Vulnerability: EDPU trusted data verification (integrity)*
- *EDPU airspeed and altitude logic (algorithm) is compromised Critical Program Information (CPI).*
  - *a. Potential Vulnerability: Operational Flight Program (OFP) containing CPI not protected by encryption*
- *EDPU receives correct airspeed and altitude inputs from MAU.*
- *EDPU applies faulty logic to MAU input, sends incorrect info to display*
  - *a. Potential Vulnerability: OFP containing CPI not protected by encryption*
- *Aircrew observes incorrect airspeed and altitude data.*
- *Air Drop (personnel and cargo), Air/Land (Take-off, en-route, landing) effectiveness degraded.*

- **Determine Vignette Priority Level**

Time and resources may not permit all potential vulnerabilities exploited in the Attack Path Vignettes to be remediated, mitigated, or tested. As such, the Attack Path Vignettes should also be prioritized for follow-on risk reduction efforts (i.e., remediation and/or mitigation) and test. The primary method of prioritization is by the associated cyber risk; however, the risk ratings are only one factor that influences vignette prioritization. While high-risk vignettes typically become high priorities, other factors may raise lower risk combinations to a higher priority. Use the considerations outlined in the following list to determine the priority level for each Attack Path Vignette.

After generating each Attack Path Vignette, transfer the key vignette details to the Attack Path Vignette Summary Table in Attack Path Analysis Report. Populate each row with data from the Attack Path Vignettes. Begin with the fields for Vignette Identification Number, Name, Attack Path, Mission Effect and Potential Vulnerabilities. As there may be multiple attack paths for each vignette, the Attack Path Vignette Summary Table may become complex. Table C-11 provides an example of what the Attack Path Vignette Summary Table might look like at this step in the process. The Table will be updated after executing the APE and determining the Attack Path Vignette Cyber Risk Score and Priority Level.

During the APE, each vignette will be analyzed further, updated to reflect the additional analysis performed, and expanded to include risk and priority ratings. The remaining Sections of the Attack Path Vignettes (i.e., MIA and Justification, Likelihood Analysis and Justification, Test Methodology, and Recommended Remediation and Mitigations) and Attack Path Summary Table (i.e., Vignette Priority, Vignette Priority Justification, and Vignette Risk Rating) will be completed during the APE.

NOTE: These are not exhaustive and are provided to help guide prioritization efforts:

- *Does the vignette include a stakeholder's Special Interest Item?*
- *What is the anticipated effectiveness of security protections in place to prevent cyber-attack entry into the system?*
- *Where is the software developed (e.g., military software foundry, US company, non-US company)?*
- *What is the security level of personnel involved with hardware and software generation?*
- *Are background checks or security clearances required for all personnel involved in the design, development, assembly, and shipment of the system?*
- *Have the system components or software been proliferated or easily acquired by an adversary?*
- *What level of security is provided to protect intellectual data related to the components (e.g., stored in secure Government network, stored in unclassified commercial system, risk of exfiltration)?*

- *What is the degree of system dependency on external systems?*
- *Is the software product hosted in a Cloud, on premise, or in a hybrid environment?*
- *Does the system utilize hardware or software controlled by a foreign or domestic third party?*
- *Are the Cybersecurity protections implemented on interfacing outside systems expected to be sufficient to prevent cyber-attacks on the SUT through the data interface?*
- *What interfacing system vulnerabilities may be inherited by connecting to that system?*
- *Is there a high level of stakeholder interest in testing the vignette, or components in the vignette?*
- *Does the vignette apply to multiple platforms?*
- *Is there interest in testing the effectiveness of defensive cyber operations for the system that would protect against execution of the vignette?*
- *Is there evidence of attempted or successful vulnerability exploitation in similar systems?*
- *Have the identified known or potential vulnerabilities identified in the vignette been mitigated?*
- *Have the identified known or potential vulnerabilities identified in the vignette already been tested? If so, is a significant change in test results anticipated?*

Table C-11   Attack Path Vignette Summary Table

Vignette Priority	Vignette Priority Justification	Risk Rating	Number	Name	Attack Path	Mission Effect	Potential Vulnerabilities
			1	Malicious Logic Injection via PCMCIA/EDPU	PCMCIA, HUMS, EDPU, Display	Compromised airspeed and altitude data accepted by aircrew, resulting in air drop being performed out of parameters (data integrity). Ineffective equipment drop results in warfighter not receiving critical supplies. Ineffective personnel drop results in injury to personnel and troops landing in incorrect location.	• PCMCIA Supply Chain compromise • No PCMCIA authenticity verification • HUMS trusted data verification (integrity) • HUMS trusted data verification (integrity) • EDPU trusted data verification (integrity) • OFP containing CPI not protected by encryption • OFP containing CPI not protected by encryption

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

APPENDIX D

ATTACK PATH ANALYSIS

Version 4.0

26 July 2021

Table of Contents

Table of Tables

FOREWARD

“Attack Path Analysis” introduces the test and evaluation methods for the cyber threats and their deterministic attack paths through the use Attack Path Vignettes to the reader.

Record of Changes

Version	Effective	Summary
4.0	26 July 2021	Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	Addition of Space Systems into SSE requirements assessment process.
3.0.1	5 November 2021	No changes to content, just updated revision numbers to correspond with body of the main document.

1.0. Background.

The Attack Path Analysis (APA) focuses on:

- Where the threat (e.g. attacker) can gain access to the system/subsystem.
- Which paths can be used to attack/exploit the system (targets are typically CPI that could cause a significant impact to missions, MCFs, and/or SCFs, if compromised).
- What the potential mission effects are if the identified potential system vulnerabilities are exploited.

It builds upon and uses the information documented in the FTA. As part of the APA, Attack Path Vignettes (APV)[43] are generated which combine identified potential cyber vulnerabilities into cyber attack scenarios. The APVs are then further analyzed and refined during an Attack Path Exercise (APE)[44].

Following the APE, test methodologies are developed for each APV, potential remediations/mitigations are determined for identified potential vulnerabilities, and an APA Report is generated. Key APV information, including the risk rating, priority rating, and attack path nodes, will be captured in the APV Summary Table.

NOTE: More information on the APE can be found in the United States Air Force's: "**Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook."**

Attack paths should be assessed based on risk. This includes analyzing the likelihood of occurrence based on a known threat and/or its projected capabilities to execute an attack (i.e., is the attack technically feasible). It includes analyzing the consequences of an attack including the impacts to a given mission.

Detailed information on how to conduct a risk assessment is located in Appendix A of this SSECG, Section 1.10.

The APA should be updated following any design changes (e.g. Engineering Change Proposals [ECP] or Configuration Control Board [CCB] decisions) that may impact potential attack paths through the systems or significant threat intelligence updates which impact the likelihood of vulnerability exploitation. Additionally, the APA should be updated after conducting any cyber test that invalidates previous attack path theories or discovers previously undocumented paths into or through the weapon or business system. Several examples of similar occurrences within a program are provided in the United States Air Force "Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook."

Appendix D provides guidance on how the APA uses the results of the FTA and the APV Template documentation to identify obvious potential vulnerabilities within the system under analysis. It is likely not cost effective to explore every possible attack path throughout a space and weapon system in every conceivable operationally specified mission; but using risk assessments, the high-risk EAPs with attack

[43] "7.2 Attack Path Vignettes", p. C-16.

[44] United States Air Force, "Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook", Version 2.0, 1 April 2020.

sources, the attack vectors to the EAP, and plausible paths through the system to the previously identified CC/CPI or critical functions mapped to the EAP combinations can be studied, and hopefully mitigated or their Cyber Survivability predicted. So, focus limited resources on creating vignettes for the greatest risks to the space and weapon system's critical functions.

2.0. Documents to review.

All available system architecture and requirements documentation (e.g. **APV Template**) should be reviewed prior to conducting the APA. While the actual documents available will vary by program and where the program is in its acquisition lifecycle, Table D-1 provides a quick look at what documents should be available at major Milestone Decision Authority (MDA), SETR and programmatic decision points. The absence of these desired documents should not prevent the execution of the APA, but may require the SSWG members to make informed assumptions about the system architecture and/or its performance based upon system requirements, other documentation, and/or similar systems.

Table D-1 Documents to Review in Support of Decision Points

	MS-A	SRR	SFR	PDR	MS-B	CDR	Post CDR
Completed FTA	X	X	X	X	X	X	X
CONOPS/CONEMP	X	X	X	X	X	X	X
[Draft/Approved] Available system requirements documents (e.g., IS-CDD, SRD, CPD, FRD)	X	X	X	X	X	X	X
Interface Control Document		X	X	X	X	X	X
Specifications (System, Sub-System), LRU, H/W, S/W, component, etc. …			X	X	X	X	X
Interface Control Documents and Data Flows			X	X	X	X	X
Completed system level and Sub-System level architectures			X	X	X	X	X
OV-1: High-Level operational concept Graphic	X	X	X	X	X	X	X
OV-2: Operational Resource Flow Description			X	X	X	X	X

	MS-A	SRR	SFR	PDR	MS-B	CDR	Post CDR
SV-4: Systems Functionality Description			X	X	X	X	X
SV-5: Operational Activity to System Function Traceability Matrix		X	X	X	X	X	X
SV-6: Systems Data Exchange Matrix		X	X	X	X	X	X
Architecture functional models			X	X	X	X	X
Failure Modes Effects and Criticality Analysis (FMECA) (reference CDRL 19 in Appendix A: USAF SSE Acquisition Guidebook, Attachment 2)				X	X	X	X
Anti-Tamper Plan/ Reports				X	X	X	X
Program Protection Plan (PPP)			X	X	X	X	X
Program Protection Implementation Plan (PPIP)			X	X	X	X	X
Safety Criticality Analysis	X	X	X	X	X	X	X
Interface Control Document				X	X	X	X
Cyber Boundary Diagram(s)	X	X	X	X	X	X	X
Available Intelligence/Threat Information	X	X	X	X	X	X	X
Fault Tree Analysis				X	X	X	X
Security Classification Guide	X	X	X	X	X	X	X

The APV data is critical in not only developing the **Cyber T&E Strategy** and in the PPP under Cybersecurity Strategy, but helping to shape requirements, design changes, mitigations, risk management, programmatic decisions, and operator and exploitation recovery procedures. Further, the information contained within the APVs become the foundation for Developmental and Operational

Testing of articulating components and potential vulnerabilities during cyber test events, such as the MBCRA and the mission effects that the testers will attempt to achieve during adversarial cyber testing.

As the design of the system matures and as a deeper understanding of the system vulnerabilities are gained, the FTA and its resultant APA will be updated iteratively throughout the development, manufacturing and fielding program milestones. For a product or service modification, the knowledge of the current baseline system's architecture and known vulnerabilities can be leveraged before the details of the modification's components are known.

3.0. APE Execution

The **APE** is a simulated table-top wartime operation that introduces and explores the effects of offensive cyber operations on the capabilities of the system to effectively perform intended mission functions in a contested cyber environment. This process expands the previously conducted analysis to incorporate cyber vulnerabilities introduced to the system by the SoS, additional SME inputs, as well as, the secondary and tertiary effects of vulnerability exploitation. During the APE, each APV will be analyzed further, updated to reflect the additional analysis performed, and expanded to include risk and priority ratings.

It is a best practice to not reveal the APVs to Operational Team members who were not involved with their generation prior to exercise start. Operational Teams that are aware of Opposing Force Team Attack intentions prior to execution have a tendency to inadvertently (or intentionally) adjust operational scenarios and/or conditions to thwart the attacks thereby reducing the exercise effectiveness.

The APE may be conducted at any point during system analysis, but is most successful when executed after completing the FTA and developing APVs. Constructive interaction between exercise participants is essential to a successful APE. The Exercise Facilitator, along with the leads from each team, must foster a positive, non-adversarial environment. The Operational Team is also strongly encouraged to identify and explain opportunities the Opposing Force Team should consider for disrupting the Operational Mission. The Operational and Opposing Force Teams working together will have a better chance of fully assessing the likelihood of success for each attack, the possible mission effects, and where system requirements and/or design adjustments are appropriate to ensure a cyber-survivable system is delivered to the warfighter.

The Exercise Facilitator and Control Team Lead monitor these discussions between the Opposing Force and Operational Teams to ensure that both sides are listening to each other and that neither team is deviating from the goal of characterizing the system (e.g., getting too far down the road or trying to "win the war" instead of exploring the potential for vulnerability exploitation, potential effects, and recommendations to design out the vulnerability or mitigate its effects). Note takers will also keep notes documenting any recommendations/ideas discussed during the exercise that would drive a more secure system. The Exercise Facilitator or Control Team Lead should table lengthy, distracting exchanges and encourage the participants to revisit them during a break or post-exercise analysis. Note takers should also be empowered to ask clarifying questions or pause discussions during the exercise in order to accurately capture the information.

At the completion of each vignette's discussion, the APE participants will make any necessary Attack Path Vignette and FTA updates, and then determine and document the Attack Path Vignette's cyber risk rating. When all Attack Path Vignettes are briefed for the given mission, the Operational Team presents the next operational mission and the process is repeated until all operational missions and vignettes are presented and discussed. Some Attack Path Vignettes may be repeated for multiple mission scenarios if a given attack path could be used to cause an effect that would impact the subject mission scenario (e.g., changing different data on a CC, exfiltration of data versus corrupting it). Once the last vignette is discussed, the Vignette Priority is determined for each Attack Path Vignette.

The classification level(s) needs to be well understood when presenting attacks as, in some cases, specific vulnerabilities, techniques against systems, or tactics associated with specific nation states will increase the classification level of the discussion. The Control Team should establish the expected level of detail for attacks and provide appropriately classified computer systems for product generation and data storage at the start of the APE to avoid classification level breaches.

3.1. APE Team

The APE utilizes the Control (White), Operational (Blue), and Opposing Force (Red) teams to perform additional vulnerability analyses, focusing on the areas deemed highest risk and/or highest priority by the cyber risk assessment team. The cyber risk assessment team members are divided into these three teams based upon their respective expertise and knowledge areas.

The Control Team coordinates and manages the exercise, identifies participants, sets goals and objectives, organizes deliverables, mediates issues, and facilitates the overall exercise. The Control Team is also responsible for taking notes during the exercise, capturing recommendations, documenting adjustments to correct incorrect or incomplete information, and performing adjustments to the APVs upon completion of each vignette discussion. The Control Team also ensures discussed test methodology, design changes, risk mitigations, attack symptoms, and attack recovery procedures are captured.

The Operational Team conducts and defends the operational mission. Prior to an APE, they develop notional plans to execute operational mission orders and achieve operational objectives within the identified timeline and scenario (typically based upon the CONOPS or CONEMP). The Operational Team also presents the notional timeline, actions, and procedures of the mission, including mission planning through post mission tasks and maintenance. The Operational Team also assesses the impact to mission accomplishment of successful cyber-attacks, assists with analysis following each scenario, provides recommendation inputs, and helps make adjustments to the FTA, APVs, and Test Methodology.

The Opposing Force Team presents the APVs in an effort to compromise data confidentiality, integrity, and/or availability in order to cause a mission impact. An effective Opposing Force Team is familiar with available system architecture, system intelligence information, and the operational mission sequence. They lead discussions of cyber-attacks to execute the Cyber Opposing Mission Objectives, provide recommendation inputs, and assist with adjusting the FTA, APVs, and Test Methodology.

After establishing the teams, APE participants must review and become familiar with available system information. The greater the detail of available information related to system design, data flows (internal and with external systems), critical system data/information, critical components, and intended operational utilization, the greater the potential return from the exercise. Information sources for review include: the PPP; boundary, DoDAF, and architecture diagrams; FTA; APA (if available); Attack Path Vignettes; CONOPS/CONEMP; relevant system and threat information; previous cyber assessment/test reports; and other applicable system documents. Prior to execution of the APE, each team will develop a tailored presentation to be delivered on day one of the event. Presentation templates are available in Appendix J.

3.2. Exercise Execution Kick-off

The formal APE begins with the Control Team presenting a briefing to the Operational and the Opposing Force Teams covering the purpose, exercise description/sequence of events, Rules of Engagement, goals, objectives and desired end state of the APE. Next, the Operational Team presents mission scenarios developed from the CONOPS/CONEMP generated during the exercise planning stage. This team explains how the mission will be conducted, from planning through mission completion, to include data flow information when available (e.g., mission planning uploads, COMSEC key loading, LINK-16). Finally, the intelligence community is afforded an opportunity to inform the participants on relevant cyber threats to the system.

3.3. Exercise Execution

APE execution begins with the Opposing Force Team presenting the Attack Path Vignette(s) that are applicable to one of the aforementioned missions, identifying the targeted system, goal of the attack, attack vector from the attack source to the platform, the attack path through the platform, the desired effect(s), likelihood assessment, any assumptions made, when the attack could be executed, and when the effects of the attack are expected to be realized. The attack may target a specific mission phase or transpire over the course of the entire mission.

Following each attack presentation, the Operational and Opposing Force Teams discuss the hypothesized path(s) through the system, system effects, the likelihood of Opposing Force Team success, and potential mission effects of the attacks. The Teams should also deliberate about critical mission areas and what opportunities those critical mission areas provide for a potential adversary.

The Operational Team will then take control of the discussion and address design changes/workarounds that could prevent or mitigate the effects of the attacks presented. Attack barriers identified by the exercise participants should drive discussions of alternate paths through the system enroute to the target component. Discussions about recovery times and procedures should also be conducted to fully comprehend the system's capability to perform the mission critical tasks or functions and evaluate system resiliency.

Table D-2 Typical Attack Path Exercise Team Composition

Team	Composition
Control Team (White Team)	• Control Team Lead (Facilitator): Typically Cybersecurity Subject Matter Expert (SME) or PM with a background in vulnerability assessment and offensive Cybersecurity operations • PM • Cybersecurity SME • System Lead Engineer • Note takers
Operational Team (Blue Team)	• Operational Team Lead: Typically system SME from PMO (or contractor) • Military and Civilian personnel from DT and OT organizations • Operational Users and maintainers with experience in the mission area of interest • Organizations already involved with the system development (POs) • Engineers familiar with the differences between the current "as is" and "to be" state of systems of interest • Subsystem SMEs • Cybersecurity SME • Cybersecurity Service Provider (CSSP)s, MDTs, CPTs, or other defense personnel for the SUT
Opposing Force Team (Red Team)	• Opposing Force Team Lead: Typically a cyber SME from the cyber test community • National Security Agency certified Red Team penetration testers (for systems connected to the DoD Information Network [DoDIN]) • Certified ethical hackers (contractors or Government personnel) • Defensive and offensive Cybersecurity SMEs • Cyber testers and analysts – preferably from the cyber test agencies likely to test the system • Cyber range (DoD, national, or commercial) personnel • Interoperability engineers • CSSPs, MDTs, CPTs, other DoD personnel for SUT • System engineers or testers

3.4. Update Attack Path Vignettes and FTA

At the conclusion of the discussion for each attack presented, the Facilitator should summarize the key data for the Note taker(s). The Note taker, assisted by the APE participants, will update the presented Attack Path Vignettes and the FTA, as required, to reflect updated information. Any Attack Path Vignette deemed invalid should be marked accordingly and placed into an archive. Information that renders the vignette invalid should be clearly articulated on the vignette so future APEs do not spend time re-investigating these vignettes. If any new attack paths are identified and discussed during the exercise, the APR participants will generate new Attack Path Vignettes at this time.

If it is determined that any of the data or risk calculations pertaining to EAPs contained in the FTA require updating to include any EAP not explored in the Attack Path Vignettes, or if new EAPs were discovered/identified, the FTA will be updated. The updates may result in the recalculation of cyber risk assessments and priority levels for some of the potential EAPs.

3.5. Information to Document in the Attack Path Analysis Report

Upon completion of the APE, the Attack Path Analysis Report will document as a minimum:

- Assessment Scope, including boundaries and interfaces evaluated.
- Subsystems/LRU/component Access Points reviewed during the FTA (include the generated connections Tables either as part of the main document or in an Appendix).
- Subsystems/LRU/EAPs/vulnerabilities assessed during the APA to include:
    - Attack Path Summary Table
    - Attack Path Vignettes
- Results of the analysis (e.g., identified vulnerabilities).
- Updated Risk Assessment per Work Breakdown Structure for the USAF SSE Cyber Workflow Process, step 4.4 Risk Assessment.
- Cyber failure modes.
- Recommended requirements, remediations, and/or mitigations for identified vulnerabilities.

NOTE: In Agile or DevSecOps software development environments, these requirements may take the form of additional or updated User Stories, Epics or backlog requirements. Any duplicated, ambiguous, untestable, infeasible, compounding, and unnecessary requirements should be removed and/or revised.

4.0. Cyber Test Methodology

Referencing the Attack Path Method section of the APVs, the cyber test team members of the SSWG Cyber Risk Assessment Team will develop the Potential Test Methodology section of each APV. This section provides the high-level approach as to how the vulnerabilities identified in the APV and the system's Cyber Resiliency will be tested, who will perform the test(s), and other cyber test details. This will in turn help inform the Cyber Test and Evaluation Strategy. Subsequently, the test team members will identify any anticipated test procedures or steps that should be taken from the EAP to the target that will evaluate the effectiveness of the cyber protections and Cyber Resiliency of the identified system components (i.e., code development, non-destructive code execution, system architecture enumeration, transmission of data via radio frequency, software installation, and data exfiltration).

Test team members will identify specific resources required to fully evaluate each potential vulnerability and component along the intended attack path. They should consider required test resources such as laboratories, cyber test asset, ranges, test equipment, personnel, hardware, software, and tools.

This same test team will identify which agencies should perform the cyber test(s) required for each vignette. Each Cyber Test Agency has an area or group of areas that it specializes in, which can force a program into using multiple independent Cyber Test Agencies to fully test all components of interest within the developmental, test, and operational environments.

The test team will identify what types of cyber testing are anticipated to properly evaluate the identified attack path (e.g., CVI, ACD, CVPA, AA, penetration, security assessment,…,) and identify when in the DoD 6-Phase process and system developmental lifecycle specific test activities should be performed.

MBCRA Verification Test, Cybersecurity Functionality Verification Test, Penetration Test, and Non-IP Device Testing will be performed during CVI and CVPA phases. Cyber Survivability Testing and Penetration Testing executed during the ACD and AA phases are used to assess a system’s cyber protections and Cyber Resiliency. The test team will identify test limitations that will hinder planned test activities while considering their factors such as interface accessibility, exploitation restrictions, software and hardware maturity, and the fidelity of documentation.

The test team will identify anticipated test risks that will impact the planned test activities while considering issues, concerns and risks such as damage to the equipment under test, corruption of the system baseline software, and the residual effects of the test data’s integrity, availability or being compromised. The team will also identify planned test mitigations to deter anticipated test risks while considering mitigations such as dedicated test assets, the use of hardware-in-the-loop laboratories, co-operative testing, non-destructive test points, and a possible technical refresh of the system prior to its testing.

5.0. Cyber Test and Evaluation Strategy

Cyber Test and Evaluation Strategy (CTES)[45] evaluates the system for Cyber Survivability through the execution of thorough Cybersecurity and Cyber Resiliency testing, ensuring that the systems delivered to the warfighter are effective and survivable in cyber contested and operational environments. To achieve this goal, cyber test activities must begin as soon as a Program-Of-Record is established and continue throughout its AAF lifecycle (i.e., beginning with cyber risk assessments and progress through adversarial assessments on the operational systems in the operational environment). The test team should be involved as soon as is practical in the early system assessments based on any available program documentation, hands-on testing of individual components/sub-components during system development, and Cyber Survivability testing of complete systems and the entire platform in test and operationally representative environments.

The CTES documents the program's incremental and integrated approach to testing Cyber Survivability during the system's development, DT&E, Operational Test & Evaluation (OT&E), and RMF controls assessments, as a minimum. It articulates what will be tested, who will perform the tests, timing, test assets, test objectives, and how the Cyber T&E 6-Phase process will be executed. The CTES, once completed, provides all the cyber test material needed for the TEMP and CSS.

Execution of the prior FTA cyber risk assessment process will help identify and prioritize system components that require Cyber Survivability testing. The process also involves developing cyber test methodologies for the generated APV that also serve as the foundation for cyber test plans. System maturity rates, component delivery timelines, test asset availability, and contract language further influence test timing and scope of cyber testing from program stand-up to sustainment entry.

The CTES should be reviewed and updated with each APA iteration or when any design, resource, or schedule adjustments are made that impact the Cyber Test Strategy. Any changes to the CTES should be reflected in the PPP and TEMP, as required. The CTES template should be included in the Cyber Risk Assessment Report.

> **NOTE:** This CTES template will be provided in this Guide's Appendix J, as soon as, a final version of the CTES template will be available in the next version of the United States Air Force, "**Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook", MRAP-C Guidebook**, currently Ver. 2.1.

For vulnerabilities that cannot or will not be eliminated through design changes, identify mitigations that may be implemented to reduce the likelihood of vulnerability exploitation and/or the potential impact if that vulnerability is exploited. This may include the implementation of additional access controls and adding protections in connecting systems if Cybersecurity related, or predicting the Cyber Resiliency of the system within its degraded mode of operation or functionality.

[45] Director Operational Test and Evaluation (DOT&E) Memo, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," 3 April 2018

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

APPENDIX E

SSE REQUIREMENTS IMPLEMENTATION ASSESSMENT

Version 4.0

26 July 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Secretary of the Air Force, Public Affairs (SAF/PA) Case #: 2021-0424. Requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

1

Table of Contents

Table of Tables

Table of Figures

FOREWARD

“SSE Requirements Implementation Assessment” introduces the assessment of how well Cybersecurity and Cyber Resiliency are being incorporated into the design/modification and development of new space and weapon systems to the reader.

Record of Changes

Version	Effective	Summary
4.0	26 July 2021	Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	Addition of Space Systems into SSE requirements assessment process.
3.0.1	29 January 2021	No changes to content, just updated revision numbers to correspond with body of the main document.

1.0. SSE Requirements Implementation Assessment.

1.1. Introduction.

During the design and development of a new space and weapon system, or modification to an existing space and weapon system, an assessment of how well Cybersecurity and Cyber Resiliency are being incorporated should be performed at various steps throughout the development. This will occur at initial requirements development, and will be updated at risk assessments and prior to SETR events. Table E-1 lists the specific WBS steps for each use of the SSE Requirements Implementation Assessment.

The PMO should perform the assessments if it has the information to do so, or include CDRL (see **Appendix A, Attachment 2**) in the RFP to have the contractor provide the assessments.

The Excel workbook embedded below provides a tool for documenting and tracking each SSE Requirements Implementation Assessment. If the processes in this guidebook are followed for decomposing the system and allocating the SSE requirements, then the majority of the inputs for the SSE Requirements Implementation Assessment Tool should be already accomplished.

SSE RQMTS
IMPLEMENTATION.xl

NOTE: Click to open the SSE Requirements Implementation Assessment Tool Excel Workbook

Table E-1 Timeline of SSE Requirements Implementation Assessment

SSECG - WBS Steps	WBS Step Description	Action	Tool
1.3.2.1	Assess SSE Requirements Implementation	Assess initial SSE Requirements Implementation	Assess the system requirements implementation (Tab 2); if doing a system modification, also assess the fielded system (Tab 1)
1.7.4	Risk Assessment	Update existing Implementation Assessment	Use the system requirements assessment (Tab 2)
2.4	Risk Assessment	Update existing Implementation Assessment	Use the system requirements assessment (Tab 2)
4.2.1	SRR	Update existing Implementation Assessment	Use the system requirements assessment (Tab 2)
4.2.3	SFR	Update existing Implementation Assessment	Use the system requirements assessment (Tab 2)
4.2.5	PDR	Update existing Implementation Assessment	Use the lower-level requirements assessment (Tab 3)
4.2.7	CDR	Update existing Implementation Assessment	Use the lower-level requirements assessment (Tab 3)
4.2.8	TRR	Update existing Implementation Assessment	Use the lower-level requirements assessment (Tab 3)
4.2.9	FCA/SVR	Update existing Implementation Assessment	Use the lower-level requirements assessment (Tab 3)
4.2.10	PRR	Update existing Implementation Assessment	Use the lower-level requirements assessment (Tab 3)
4.2.11	PCA	Update existing Implementation Assessment	Use the lower-level requirements assessment (Tab 3)
4.4	Risk Assessment	Update existing Implementation Assessment	Assess the lower-level requirements implementation (Tab 3)

1.2. Assessing Weapon Systems

1.2.1. Overview.

The process for assessing a new system is different from a modification to a current system, in that for the modification you will also have to assess the current system separate from the design for the modification, as shown in Figure E-1. This is only required for the initial assessment. All updated assessments require only assessing the modification independently.

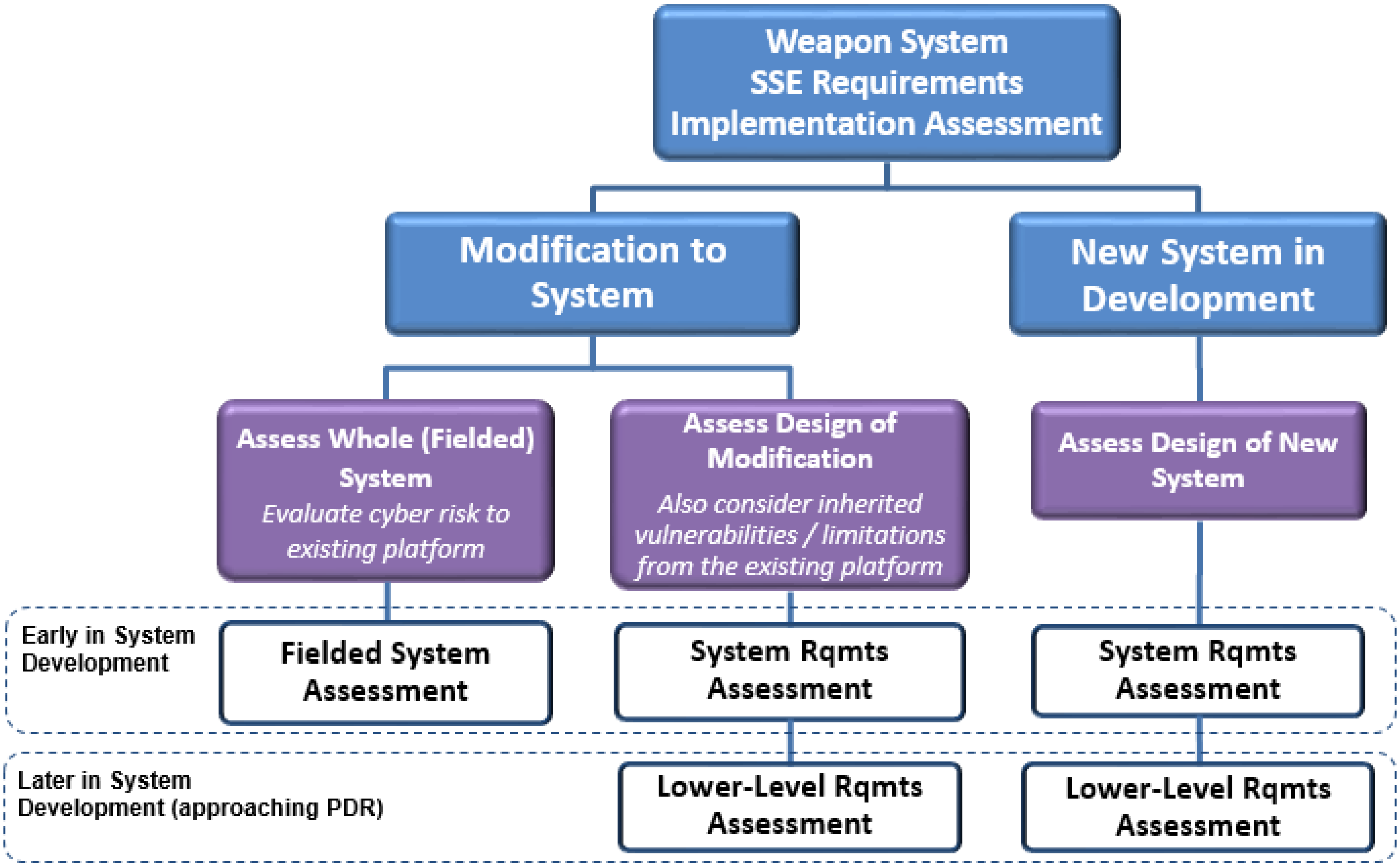

Weapon System SSE Requirements Implementation Assessment
Modification to System
New System in Development
Assess Whole (Fielded) System
Evaluate cyber risk to existing platform
Assess Design of Modification
Also consider inherited vulnerabilities / limitations from the existing platform
Assess Design of New System
Early in System Development
Fielded System Assessment
System Rqmts Assessment
System Rqmts Assessment
Later in System Development (approaching PDR)
Lower-Level Rqmts Assessment
Lower-Level Rqmts Assessment

Figure E-1 SSE Requirements Implementation Assessment.

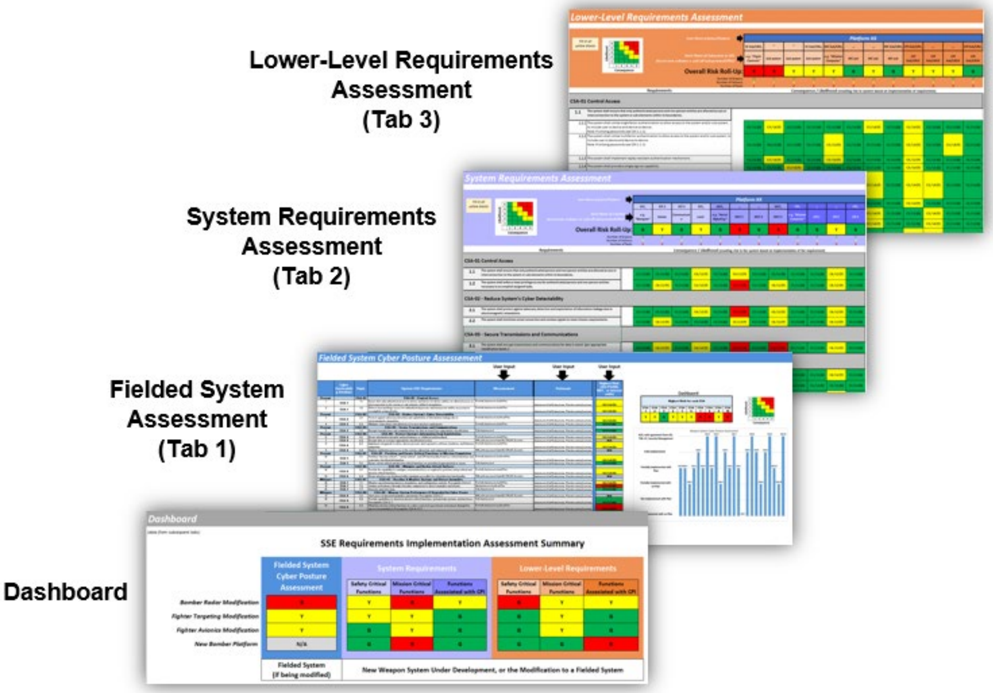
1.2.2. Modification to an Existing Weapon System.

For a system modification, first assess the existing space and weapon system platform, and then assess the modification design. Both of these assessments will use the SSE requirements within this guidebook as the basis for evaluation, although the methodology will be slightly different.

NOTE: Refer to **Appendix A: SSE Acquisition Guidebook, Attachment 1**.

The SSE Requirements Implementation Assessment Tool hierarchy is displayed by Figure E-2. Use the information in Tab 1 of the embedded Excel workbook for the SSE Requirements Implementation Assessment to perform the assessment on the existing/fielded space and weapon system first. Also, reference cyber-related risks from existing POA&Ms or NDAA 1647 assessments as needed. These identified risks are used to inform the Cybersecurity and Cyber Resiliency requirements for the modification. For example, there may be existing cyber vulnerabilities in the space and weapon system that may require additional SSE requirements within the modification to ensure it is better protected. There may also be limitations with the way the space and weapon system was designed that limit the ability to implement certain SSE requirements that were planned for the modification.

Next, assess the design for the modification using the system requirements on Tab 2 of the Excel tool. This tab will be used for updates to the assessment up through SFR. At PDR, when the system design is fully decomposed, then begin using Tab 3 to evaluate against the more specific, lower-level requirements.


Lower-Level Requirements Assessment (Tab 3)
Lower-Level Requirements Assessment
System Requirements Assessment (Tab 2)
System Requirements Assessment
Fielded System Assessment (Tab 1)
Fielded System Cyber Posture Assessment
Dashboard
Dashboard

SSE Requirements Implementation Assessment Summary

	Fielded System Cyber Posture Assessment	System Requirements			Lower-Level Requirements		
		Safety Critical Functions	Mission Critical Functions	Functions Associated with CPI	Safety Critical Functions	Mission Critical Functions	Functions Associated with CPI
Bomber Radar Modification	R	Y	R	Y	R	Y	Y
Fighter Targeting Modification	Y	Y	Y	G	G	Y	G
Fighter Avionics Modification	Y	G	Y	G	G	Y	G
New Bomber Platform	N/A	G	R	G	G	G	R
	Fielded System (if being modified)	New Weapon System Under Development, or the Modification to a Fielded System					

Figure E-2 SSE Requirements Implementation Assessment Tool

1.2.3. New System Development.

For assessing a new space and weapon system in development, skip Tab 1 and begin by using Tab 2 for the initial assessment. Continue to use this tab for all updated assessments until PDR. Prior to PDR, begin using Tab 3 with the more detailed lower-level requirements. Continue using this tab with lower-level requirements for all remaining assessment updates throughout the life of the program.

1.2.4. Dashboard.

The dashboard tab will give a summary view of the results of the analysis in the other tabs. It will display the highest risk in each Section. For example, if there is one red risk in the Section, the rolled up value on the dashboard will show red.

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

APPENDIX F

RELATIONSHIP TO OTHER PROCESSES

Version 4.0

26 July 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Secretary of the Air Force, Public Affairs (SAF/PA) Case #: 2021-0424. Requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

Table of Contents

Table of Tables

Table of Figures

FOREWARD

“Relationship to Other Acquisition Lifecycle Processes” introduces the software development environments of: Agile/Agile (SCRUM), DevOps and DevSecOps along with the Cloud technologies to the reader. It further amplifies the earlier discussion of the DoD AAF and acquisition of IT Information Services as a part of the expanded coverage of DBS within the DoD and USAF.

More importantly, it updates the latest relationships and RMF controls within the NIST SP800-53/-53b and their interplay with the existing SSEC Workflow processes related WBS Tasks/Sub-Tasks.

Record of Changes

Version	Effective	Summary
4.0	26 July 2021	Approved for Public Release; Distribution Unlimited.
4.0	1 June 2021	Introduction of software development environments and latest NIST RMF Controls workflow tasks/sub-tasks.
3.0.1	29 January 2021	No changes to content, just updated revision numbers to correspond with body of the main document.

1.0. Acquisition Lifecycle & the SSECG Workflow

In addition to the standard acquisition life cycle, the Workflow Process is related to Cybersecurity test and evaluation (specifically the Mission Based Cyber Risk Assessment), as well, as the Risk Management Framework.

Space systems require additional considerations with regards to architecture and survivability. Component criticality and SCF risk assessments require that the SSWG include an Astrodynamicist and Astrophysicist along with material science experts to deal with the Cyber Events unique to the hostile space environment. With regards to SSE, SMC-TR-05-02 is germane, along with the existing engineering best practices in place at Space Command Control (SCC).**SSE Cyber Workflow Process and Adaptive Acquisitions Framework (AAF)**

2.1 Urgent Capability Acquisition Pathway

DoDD 5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs*, and DoDI 5000.81, *Urgent Capability Acquisition*, establish policies and provide procedures for the DoD's highest priority providing warfighters with capabilities urgently needed to overcome unforeseen threats, achieve mission success, and reduce risk of casualties. Urgent operational needs and other quick reaction capabilities are identified and approved for resolution by designated authorities. The acquisition; product support and sustainment processes; reviews; and documents are aggressively streamlined due to operational urgency. The goal is to plan for the capability in a few weeks, and with development and production measured in months. The SSE Cyber Workflow Process provides the PM the flexibility to effectively execute this pathway.

The urgent nature of this pathway does not forego Cybersecurity and other protection measures as stated in DoDI 5000.81, 4.3 (b):

"(1) Development includes an assessment of the performance, safety, suitability, survivability, supportability, including software, and lethality, if appropriate. It does not require that all identified deficiencies including those related to safety be resolved prior to production or deployment. The MDA will, in consultation with the User community and the requirements validation authority, determine which deficiencies must be resolved and what risks can be accepted. The accepted risks will allow the User community to develop tactics, techniques, and procedures to help minimize the operational risks.

(2) IT, including National Security Systems, fielded under this issuance require an authorization to operate in accordance with DoDI 8510.01. DoD Component chief information officers will establish processes consistent with DoDI 8510.01 for designated approval authorities to expeditiously make the certification determinations and to issue interim authorization to test or authorization to operate."

For programs executing this pathway, it is recommended to conduct the Functional Thread Analysis (FTA), as well as, the Attack Path Analysis (APA) within Appendix C and D of this guide, at a minimum. These two analyses will provide critical information regarding system architectures and cyber vulnerabilities, so that the program can take appropriate actions to mitigate risks.

2.2 Rapid Acquisitions / Middle Tier for Acquisition Pathway

The Middle Tier for Acquisition (MTA) pathway (established by Section 804 of the National Defense Authorization Act for Fiscal Year 2016) allows for rapid fielding or rapid prototyping that cannot be accomplished through traditional acquisition methods. DoDI 5000.02 *AAF*, states in Section 4.1, paragraph b (3), that regardless of the acquisition pathway being used, Program Managers will address cyber risks early and continuously to ensure fielded systems are cyber resilient:

> *"b. In addition, PMs will:*
> *(3) Recognize that Cybersecurity is a critical aspect of program planning. It must be addressed early and continuously during the program life cycle to ensure Cybersecurity operational and technical risks are identified and reduced and that fielded systems are capable, effective, and resilient."*

DoDI 5000.90, clearly emphasizes Cybersecurity in its depiction of the acquisition pathways that cyber defenses are still a top priority and are not intended to be bypassed in order to "go faster".

DoDI 5000.80, "Operation of the Middle Tier of Acquisition (MTA)" directs the use and application of this pathway and states in Section 2.6, paragraph b, the PMs will:

- Ensure operational, technical, and security risks are identified and reduced so that fielded systems are capable, effective, and resilient.
- Comply with statutory requirements unless waived in accordance with relevant provisions.

DoDI 5000.80, *MTA,* states in Section 3.1, paragraph c:

> *"DoD Components will develop a process for demonstrating performance and evaluating for current operational purposes the proposed products and technologies. This process will result in a test strategy or an assessment of test results, included in the acquisition strategy, documenting the evaluation of the demonstrated operational performance, to include validation of required Cybersecurity and interoperability as applicable. Programs on the DOT&E oversight list will follow applicable procedures."*

Tailoring of the SSE Cyber Workflow Process provides the process for the PM execution control and sequencing for successful and timely program execution. Efforts should be made to include as many of the steps within the SSE Cyber Workflow Process as possible to ensure:

- Understanding of Mission Critical Functions, Safety Critical Functions, and any other functions associated with critical program information
- Inclusion of SSE requirements in the programs contract(s)
- Execution of the Functional Thread Analysis (which supports previous bullet)
- Execution of the Attack Path Analysis
- Risk assessments that evaluate cyber vulnerabilities and consequences of cyber incidents/attacks
- Verification of SSE requirements (through both testing and technical/progress reviews)

2.3 Major Capability Acquisition Pathway

This acquisitions pathway is the traditional program adhering to DoDI 5000.01, "*The Defense Acquisition System",* and DoDI 5000.85, "Major Capability Acquisition". They are designed for supporting major defense acquisition programs, major systems, and other complex acquisitions. The SSE Cyber Workflow Process developed around this pathway typically follows a structured analyze, design, develop, integrate, test, evaluate, produce, and support approach where acquisition and product processes are tailored based on the program size, complexity, risk, urgency, and other factors.

2.4 Software Acquisition Pathway

The Software Acquisition Pathway integrates modern software development practices such as Agile Software Development (Figure F-1), Security, and Development Operations (DevOps) displayed in Figure F-2, and Development Security Operations (DevSecOps)[46], Figure F-3, that are normally executed in parallel and subsumed within another pathway. Software programs that meet the definition of a Defense Business System (DBS) and primarily acquire Commercial-Off- The-Shelf (COTS) components will follow DoDI 5000.75 procedures but may elect to use this pathway for custom developed software. DoDI 5000.02 AAF, states in Section 4.1, paragraph b (3) that regardless of the acquisition pathway being used, the PM addresses cyber risks early and continuously ensuring fielded systems are cyber resilient:

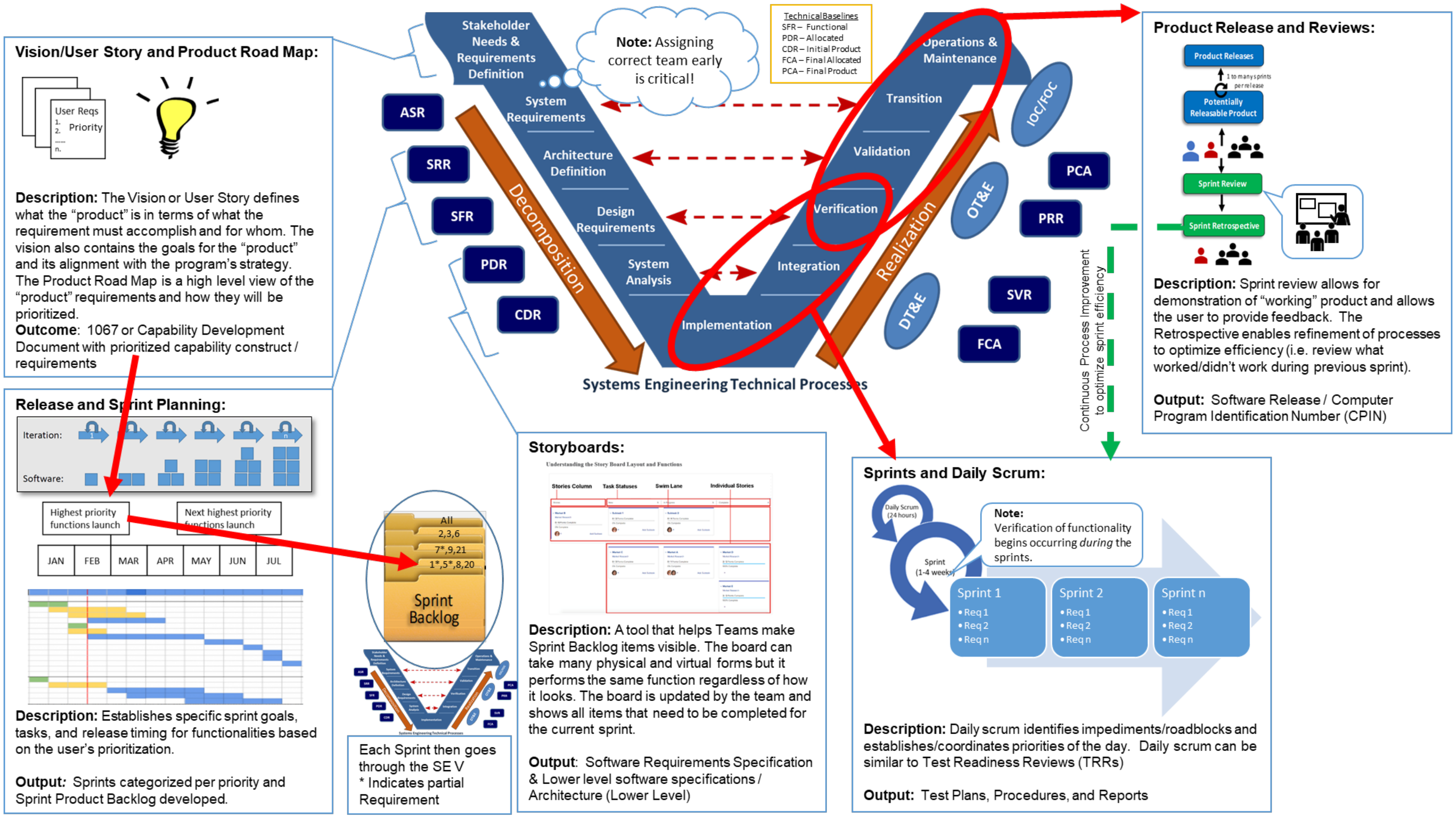
> *"b. In addition, PMs will:*
> *(3) Recognize that Cybersecurity is a critical aspect of program planning. It must be addressed early and continuously during the program life cycle to ensure Cybersecurity operational and technical risks are identified and reduced and that fielded systems are capable, effective, and resilient."*

IAW Under Secretary of Defense, 03 Jan 2020, Memo, Software Acquisition Pathway Interim Policy and Procedures, Policy Items:

" g) The PM shall ensure that software teams address persistent Cybersecurity requirements starting at program inception and include a risk-based lifecycle management approach to secure development, secure capabilities, and secure lifecycle to address software vulnerabilities. The PM shall also ensure that automated test processes, tools and/or environments are certified by the test community and the automated test process includes, to the greatest extent practicable, frequent and recurring tests that address cyber and software assurance considerations throughout the software lifecycle. The automated build scripts and test results shall be available to Government testers, so they can reuse/recreate any test artifact.

[46] DoD Enterprise DevSecOps Reference Design. V2.0, March 2021.

j) The PM, in collaboration with developmental and operational test organizations, shall seek to streamline, automate and integrate contractor test, Developmental Test and Evaluation (DT&E), and Operational Test (OT). The test and User communities shall participate in early program development and test planning activities. The software build and automated test process and associated data should be leveraged to enable timely satisfaction of DT and OT test criteria and User acceptance."



Vision/User Story and Product Road Map:

Description: The Vision or User Story defines what the "product" is in terms of what the requirement must accomplish and for whom. The vision also contains the goals for the "product" and its alignment with the program's strategy. The Product Road Map is a high level view of the "product" requirements and how they will be prioritized.

Outcome: 1067 or Capability Development Document with prioritized capability construct / requirements

Release and Sprint Planning:

Description: Establishes specific sprint goals, tasks, and release timing for functionalities based on the user's prioritization.

Output: Sprints categorized per priority and Sprint Product Backlog developed.

Each Sprint then goes through the SE V

* Indicates partial Requirement

Storyboards:

Description: A tool that helps Teams make Sprint Backlog items visible. The board can take many physical and virtual forms but it performs the same function regardless of how it looks. The board is updated by the team and shows all items that need to be completed for the current sprint.

Output: Software Requirements Specification & Lower level software specifications / Architecture (Lower Level)

Sprints and Daily Scrum:

Description: Daily scrum identifies impediments/roadblocks and establishes/coordinates priorities of the day. Daily scrum can be similar to Test Readiness Reviews (TRRs)

Output: Test Plans, Procedures, and Reports

Product Release and Reviews:

Description: Sprint review allows for demonstration of "working" product and allows the user to provide feedback. The Retrospective enables refinement of processes to optimize efficiency (i.e. review what worked/didn't work during previous sprint).

Output: Software Release / Computer Program Identification Number (CPIN)

Figure F-1 The Agile Workflow Process

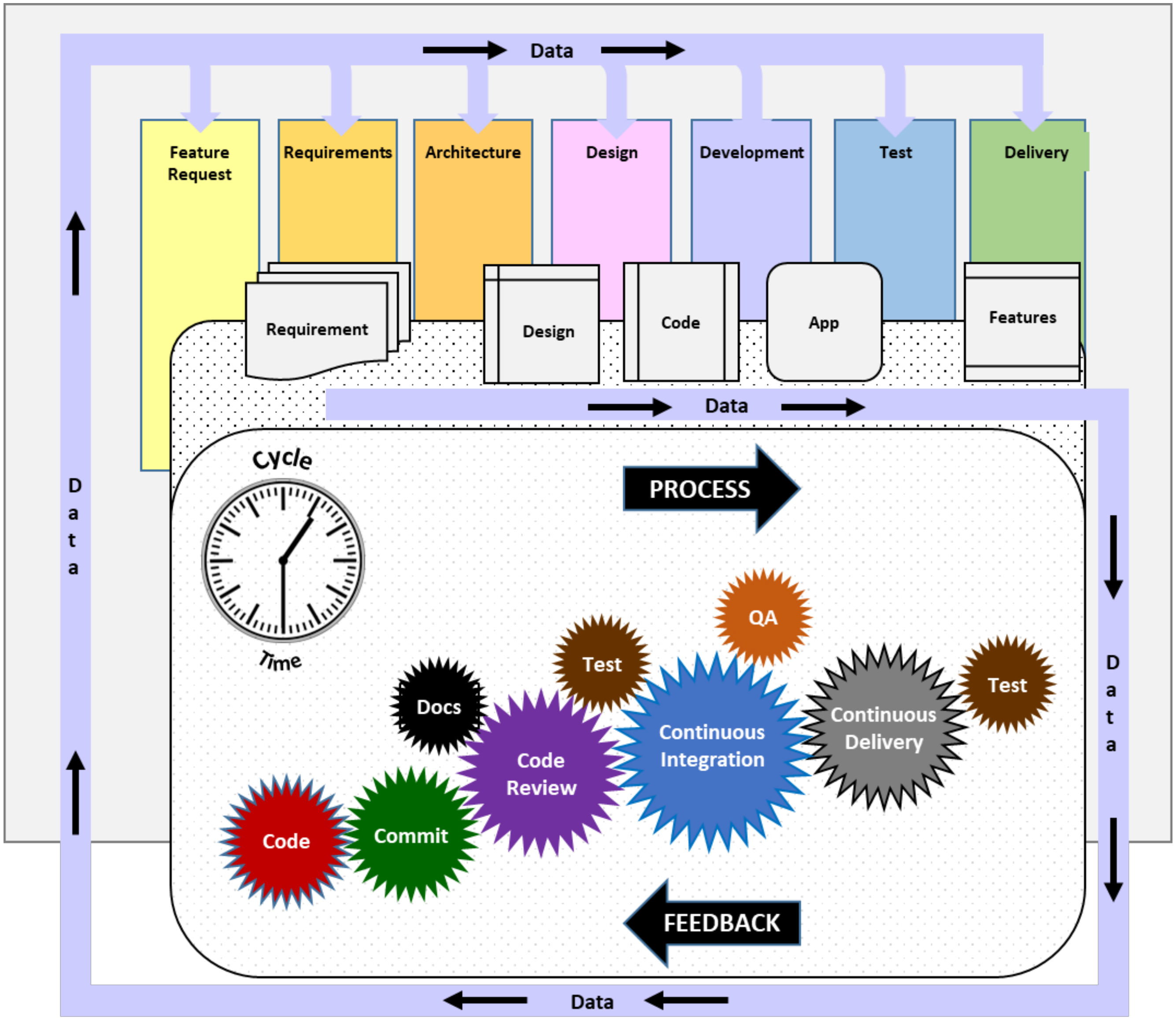


Figure F-2 DevOps Development Pipeline and the SDLC

At a minimum, programs need to ensure the following:

- Understanding of Mission Critical Functions, Safety Critical Functions, and any other functions associated with critical program information
- Inclusion of SSE requirements in the programs contract(s)
- Execution of the Functional Thread Analysis (which supports previous bullet)
- Execution of the Attack Path Analysis
- Risk assessments that evaluate cyber vulnerabilities and consequences of cyber incidents/attacks
- Verification of SSE requirements (through both testing and technical/progress reviews)

A comprehensive set of Space System software acquisition best practices has been developed based on experiences from the space systems domain. This set of software acquisition best practices was synthesized from the experiences supporting the United States Air Force (USAF), Space and Missile Systems Center (SMC), and the National Reconnaissance Office (NRO) in the acquisition of software-intensive space systems over a 20-year period. The recommended set of 24 space system software acquisition best practices is organized into ten categories to address pre-contract award activities, post contract award activities and activities performed throughout the entire pre and post-contract award periods.

These best practices for Space Systems software acquisition are not intended to be a tutorial in the application of these best practices; the rationale for their inclusion and essential elements for their effective application within the Space Systems architecture and their procurement and sustainment.

These recommended software acquisition best practices are not independent of each other; in fact, effective use of a particular software acquisition best practices are to be used concurrently with other software acquisition best practices in one of the AAF lifecycles.

3.0. DevSecOps

DevSecOps combines software development and operations to shorten development cycles, allowing organizations to be agile, and maintain the pace of innovation while taking advantage of cloud-native technology and practices.

Industry and Government have embraced and are rapidly implementing these practices to develop and deploy software in operational environments, often without understanding and considering of security.

DevSecOps helps ensure that security is addressed as part of all DevSecOps practices by integrating security practices, and automatically generating security and compliance artifacts throughout the process. This is important for several reasons, including:

- Reduces vulnerabilities, malicious code, and other security issues in released software without slowing down code production and releases.
- Mitigates the potential impact of vulnerability exploitation throughout the application lifecycle, including when code is being developed and software is executing on dynamic hosting platforms.
- Addresses the root causes of vulnerabilities to prevent recurrences, such as strengthening test tools and methodologies in the toolchain, and improving practices for developing code and operating hosting platforms.
- Reduces friction between the development, operation, and security teams in order to maintain the speed and agility needed to support the organization's mission while taking advantage of modern and innovative technology.

3.1 DevSecOps Management Difficulties

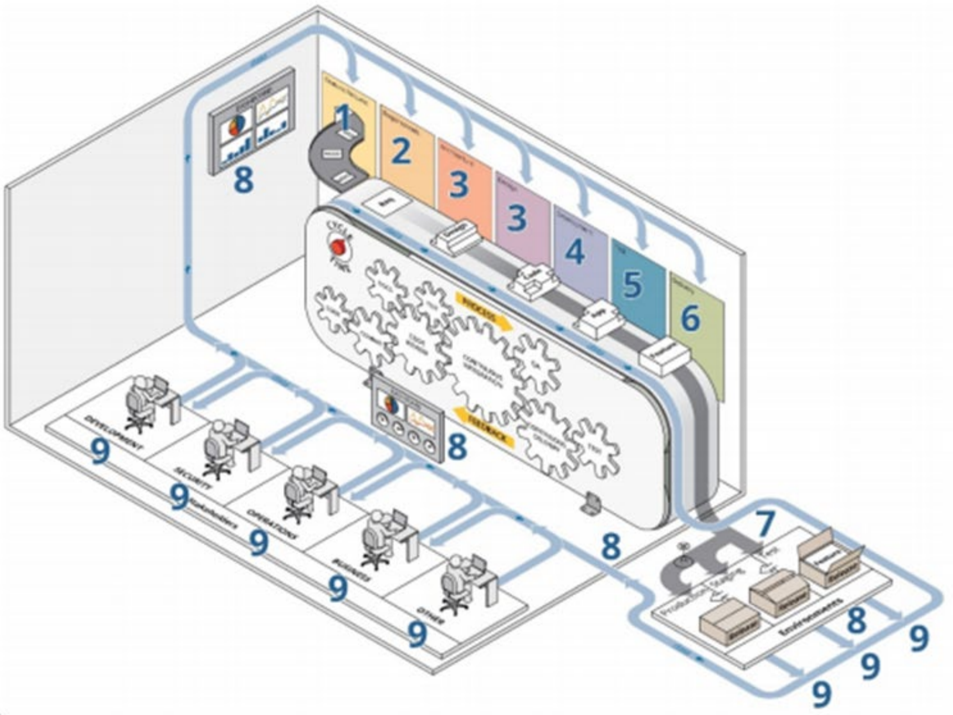
DevSecOps requires some careful forethought when writing a Software Development Plan (SDP). As with any new software methodology, space and weapon systems being CPS architectures composed of SoS pose unique challenges for fashioning contracts that allow transparent and purposeful management of the DevSecOps workflow processes, namely:

- Individuals with different security clearances impairing collaboration
- Permissions for development, integration, testing and management tools not uniform across the entire DevSecOps organization
- Infrastructure-as-Code (IaC) have restricted access for Developers
- Authority-To-Operate (ATO) hampered by the enclaves segregated due to data and tool classification levels
- Updating of data and tools across the segregated development enclaves

3.2 DevSecOps Contractual Problems

Within a Contractor/ Program Office multi-discipline team problems stemming from cross-functional reporting, multiple project stakeholders and constant delivery pressures - the issues are never-ending. It is difficult enough to get everyone on the same page not to mention the technical and contractual issues involving human resources. Areas for increased emphasis within a contract using DevSecOps should address contemporary historical problems of:

- The Release Manager's lack visibility into the daily workflow process
- Lack of visibility for the overall end-to-end workflow
- Sacrificing code quality for speed
- Sacrificing development quality for speed
- QA Manager not tracking development or code quality
- Difficulty in tracking code development against contractual requirements
- DevSecOps Manager has limited workflow controls
- Development environment has limited workflow controls
- The Release Manager has poor coordination within the other program teams
- Poor Program Management team/resource coordination
- The Release Manager has a poor audit trail process or tool
- The audit trail lacks adequate detail for Government insight and development tracking



1 Feature Request

- Strategy & Metrics
- Policy & Governance
- Education & Security Guidance
- Organizational Risk Factors
- Threat Assessment

2 Requirements

- Security Requirements (SFR/SAR)
- Risk Assessment
- Abuse Case Development
- Threat Modelling
- Security Stories
- Screen Development Tools
- Secure/Hardened Environments

3 Architecture & Design

- Security Architecture
- Architectural Risk Analysis
- Security Design Requirements
- Attack Surface Analysis
- Threat Modelling
- Vulnerability Analysis and Flow Hypothesis
- Security Design Review
- Dependencies List, Open-source libraries

4 Development

- Secure Coding Practices
- Security Focused Code Review
- Deprecate Unsafe Functions
- Perform Security Unit Testing
- Static Code Analysis
- Checking of process and procedures for secure coding & traceability

5 Testing

- Security Test Planning
- Security Testing
- Fuzz Testing
- Risk Based Security Testing
- Perform Dynamic Analysis
- Penetration Testing
- Verification of Security Implementation
- Verification of Process and Procedures
- Dependency Monitoring

6 Delivery

- Container Security
- Final Security Review
- Certify, Release and Archive
- Security Acceptance Testing
- Transition Incident Response Plan

7 Deploy

- Application Security Monitoring
- Secure Deployment Process
- Secure Environment
- Secure Operational Enablement

8 Data

- Mean Time to Recovery (MTTR)
- Mean Time to Detection (MTTD)
- Issue Volume and Resolution Time
- Deployment Frequency
- Change Lead Time and Volume
- Change Failure Rate
- Time to Patch Vulnerabilities
- Development and Application Logging Availability
- Retention Control Compliance
- SAR Findings
- Attack Vector Details (IP, Stack Trace, Time, Rate of Attack, etc)
- Server Disk Space, Load and Process Monitoring
- Application Performance
- Maximize Monitoring
- Change in Size to Code Base
- Most Active Code Contributors
- Most Changed Code Areas

9 All stakeholder security issues are satisfied

Figure F-3 DevSecOps Workflow Process Overview

4.0. Cloud Computing Data Storage & Security

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[47]

The various DoD implementations of Cloud architectures[48], mainly centered around data storage, entails addressing a new set of vulnerabilities that prior software development environments and data warehousing designs for the SSE and Contract Officer to consider. Whether for DBS using a Private Cloud. Community or Public Cloud architecture, or a Space or Weapon Systems employing a Community or Hybrid Cloud architecture, the cybersecurity risks depend on a high degree of outsourcing, sharing and scalability along with shared networks and data storage devices.

The NIST SP800-53, v5.0 provides many Cloud-related RMF Controls for securing Cloud components and networks; however, those dependent on outside contracted providers and services without being held to some form of CMMC (NIST SP800-171) are at great risk of exploitation.

Too many designs are relying on Cloud-based architectures due to its present popularity cult-like following and buzzword marketing factor. However, before considering a Cloud-based product or service for integration within a space or weapon system, one must consider its value as one of many other design enablers that may not be in alignment with the National Strategy for Trusted Identities in Cyberspace (NSTIC) proposed initiatives. Any AoA for a Cloud-based design should consider whether other architectures can provide[49]:

- an integrated set of security standards to secure the data and protect the privacy of the User's profile
- data, data portability, and interoperability at the software, platform, and infrastructure levels of a Cloud.

From a Cybersecurity perspective, the Program Office needs to understand that Cloud architectures demand a high degree of shared security responsibilities between the Provider and the Actor/User (See Figure F-4). The Contracted Service Provider (CSP) provides the security mechanisms, however the Program Office is responsible for activating, deploying and managing these security mechanisms (e.g. RMF Controls).

[47] NIST SP800-145, "The NIST Definition of Cloud Computing", September 2011.
[48] NIST SP500-292, "NIST Cloud Computing Reference Architecture", September 2011.
[49] NIST SP500-293, "US Government Cloud Computing Technology Roadmap Volume I, High-Priority Requirements to Further USG Agency Cloud Computing Adoption", October 2014.

4.1 Cloud Computing Contracting Considerations

Before drafting a pre-RFP set of Cloud-centric requirements, a Provisional Authorization (PA)[50] shall be performed. This pre-acquisition type of Risk Management Framework Information System Authorization used by DoD and FedRAMP to pre-qualify Commercial CSOs to host Federal Government and/or DoD information and information systems. PAs are to be used by Federal and DoD Cloud Mission Owners during source selection and subsequent system authorization under RMF.

The 15 December 2014 DoD CIO memo regarding "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services", states "components may host Unclassified DoD information that has been publicly released on FedRAMP approved cloud services." The memo also states, "FedRAMP will serve as the minimum security baseline for all DoD cloud services."

For the DoD DBS, and Space and Weapon Systems, the FedRAMP+ applies. It is leverages the work done as part of the FedRAMP assessment and adds specific security controls and requirements necessary to meet and assure DoD's critical mission requirements.

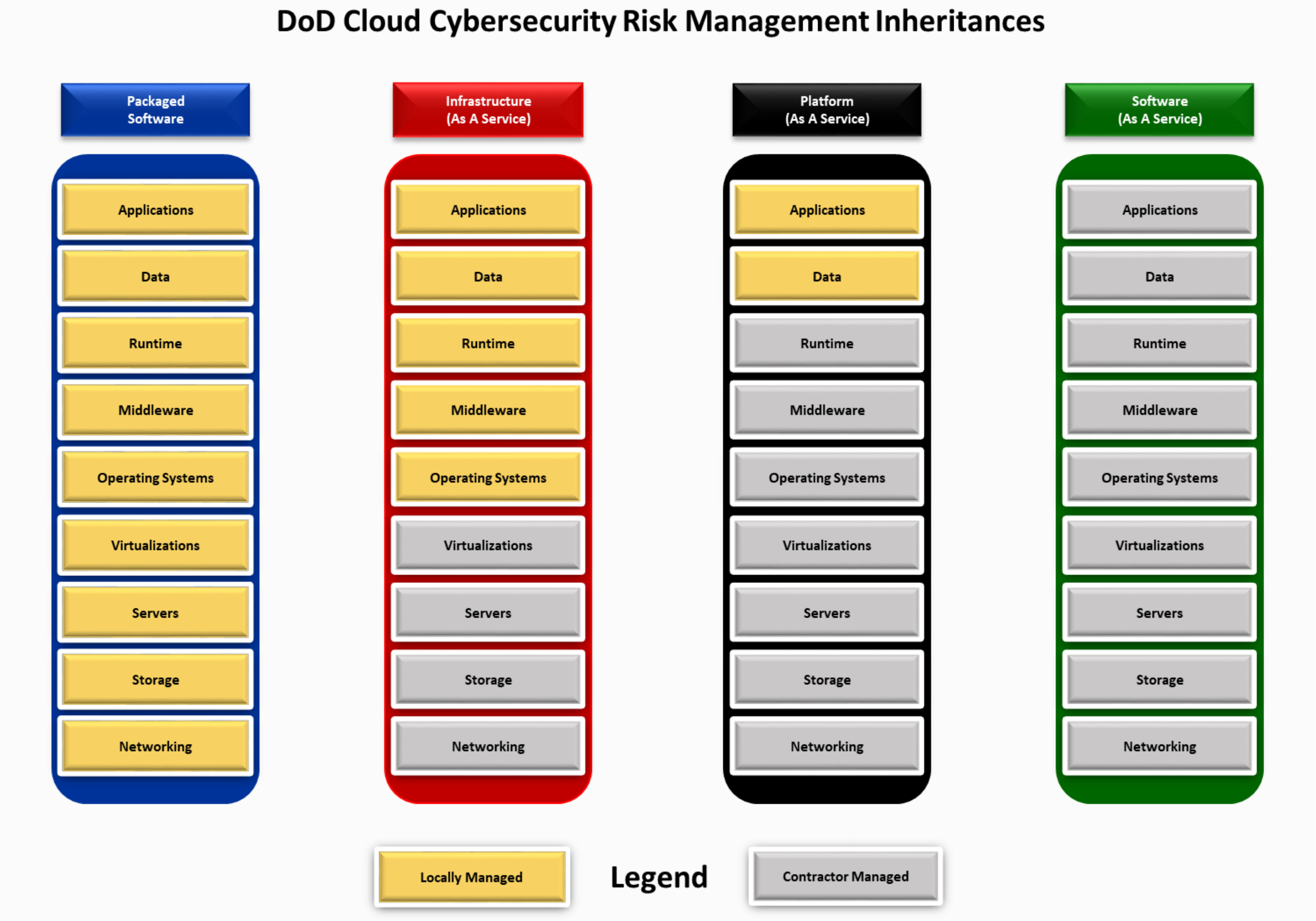
Further, this DoD CIO memorandum delineates that: "… DoD will not perform additional NIST 800-53 RMF control assessments[51] at Level 2 before awarding a DoD PA and listing in the DoD Cloud Service Catalog …"[52] For further guidance on the risk assessment on DoD Cloud-based cybersecurity objectives and cybersecurity assessment processes, and DoD-peculiar lessons-learned, refer to aforementioned "DoD Cloud Computing Security Requirements Guide" and "Best Practices Guide for Department of Defense Cloud Mission Owners"[53].

For contracting and security purposes in using a CSP for providing an Infrastructure as a Service (IaaS), the Program manager is responsible for the following components within the contract:

- Virtual Machine
- Operating systems
- Applications
- Data in transit
- Data at rest
- Databases
- Credentials to include Private Keys

[50] DoD Cloud Computing Security Requirements Guide, Version 1, Release 3, DISA, p. 31, 6 March 2017
[51] Confidentiality, Integrity, Availability
[52] DoD Cloud Service Catalog:
https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx
(DoD CAC/PKI required)
http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf
(Public)
[53] Best Practices Guide for Department of Defense Cloud Mission Owners, v1.0, 30 July 2015.

- Adhering to DoD Policies and configurations
- Vulnerability Compliance Reporting
- Data encryption for the data in transit under FIPS 140-2 or better



DoD Cloud Cybersecurity Risk Management Inheritances

Packaged Software	Infrastructure (As A Service)	Platform (As A Service)	Software (As A Service)
🟨 Applications	🟨 Applications	🟨 Applications	⬜ Applications
🟨 Data	🟨 Data	🟨 Data	⬜ Data
🟨 Runtime	🟨 Runtime	⬜ Runtime	⬜ Runtime
🟨 Middleware	🟨 Middleware	⬜ Middleware	⬜ Middleware
🟨 Operating Systems	🟨 Operating Systems	⬜ Operating Systems	⬜ Operating Systems
🟨 Virtualizations	⬜ Virtualizations	⬜ Virtualizations	⬜ Virtualizations
🟨 Servers	⬜ Servers	⬜ Servers	⬜ Servers
🟨 Storage	⬜ Storage	⬜ Storage	⬜ Storage
🟨 Networking	⬜ Networking	⬜ Networking	⬜ Networking

🟨 Locally Managed **Legend** ⬜ Contractor Managed

Figure F-4 DoD Cloud Cybersecurity Risk Inheritances

5.0. Defense Systems Capability Acquisition Pathway

The SSE Cyber Workflow Process Chart addresses USAF Weapon Systems as a National Security System (NSS) via CNSSI 1253 under NIST SP800-59 standards while DoDI 5000.75, *Business Systems Requirements and Acquisition*, and addresses a business system, as defined below:

> *"Business systems are information systems that are operated by, for, or on behalf of the Department of Defense, including: financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, human resources management systems, and training and readiness systems. A business system does not include a national security system or an information system used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the DoD conducted for the morale, welfare, and recreation of members of the armed forces using non-appropriated funds."*

Whereas, a USAF Weapon Systems Cybersecurity framework is directed by CNSSI 1253, the IT-centric NIST SP800-53 RMF is ideal for the DoD business system. DoDI 5000.75 defines Cyber Resiliency as "*An entity's ability to continuously deliver the intended outcome despite adverse cyber events*" while the SSE Cyber Workflow Process Chart states that "*Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.*"

Compared to USAF Weapon Systems, DoDI 5000.75 has no formal definition for Cyber Survivability; but the definition for Cyber Resiliency resembles the USAF Weapon System definition for Cyber Survivability.

While the USAF Weapon Systems usually processes the highest classified data and while the DoD Business is not classified, but may contain Controlled Unclassified Information (CUI), Personal Identifiable Information, Personal Health Information, Intellectual Property or FOUO data; they both must provide continuous monitoring while providing Cybersecurity program protection for their data at their respective level. They must comply with Clinger-Cohen Act and their own myriad barrage of DoD regulation addressing Cybersecurity, Cyber Resiliency, system survivability, and finally must possess an authority to operate/connect while performing continuous monitoring for maintaining their system viability. Although the exact artifacts and processes may differ, the SSE Cyber Workflow Process provides the PM a tailored flexible process for their program execution.

5.1 Acquisition of Services Pathway

DoDI 5000.74, Defense Acquisition Of Services, defines the Acquisition of Services Pathway allowing the PM to acquire services from the private sector including knowledge-based, construction, electronics and communications, equipment, facilities, product support, logistics, medical, research and development, and transportation services, such as a launch facility and is subsumed within another pathway. DoDI 5000.02 AAF, states in Section 4.1, paragraph b (3) that regardless of the acquisition pathway being used, the PM addresses cyber risks early and continuously ensuring fielded systems are cyber resilient:

> *"b. In addition, PMs will:*
> *(3) Recognize that Cybersecurity is a critical aspect of program planning. It must be addressed early and continuously during the program life cycle to ensure Cybersecurity operational and technical risks are identified and reduced and that fielded systems are capable, effective, and resilient."*

DoDI 5000.74 requires Clinger-Cohen Act (CCA) mandate compliance and within Table 2 "… *requires Cybersecurity for the IT services complies with DoD Cybersecurity policies and standards."*

Tailoring of the SSE Cyber Workflow Process provides the framework for the PM execution control and sequencing for successful and timely program execution delivering a weapons system for both the parent pathway and this child pathway.

6.0. Test and Evaluation

The SSE Cyber Workflow Process compliments the activities called out in the DoD Cybersecurity Test and Evaluation Guidebook.

Cybersecurity DT&E (CST&E) evaluates a system's mission performance in the presence of Cybersecurity threats and informs acquisition decision makers regarding Cybersecurity, resilience, and survivability. The focus of testing is system resiliency; testing assesses if the mission can avoid disruption due to system misuse. Mission Based Cyber Risk Assessments (MBCRAs) with CST&E, performed early and through acquisition life cycles, provides the PM a mission context Cybersecurity risk understanding. A summary is provided for each of the 6 phases of Cybersecurity T&E and for more information refer to the DoD Cybersecurity Test and Evaluation Guidebook.

- **Phase 1—Understand the Cybersecurity Requirements.** The purpose of the first phase is to examine the system's Cybersecurity and resilience requirements for developing an initial approach and plan for conducting CSTE.
- **Phase 2—Characterize the Attack Surface.** The purpose of the second phase is to identify vulnerabilities and avenues of attack an adversary may use to exploit the system and to develop plans to evaluate the impact to the mission.
- **Phase 3—Cooperative Vulnerability Identification.** The purpose of the third phase is to verify Cybersecurity and resilience and identify vulnerabilities and needed mitigations, which will inform system designers, developers, and engineers of needed Cyber Survivability and resilience improvements to reduce risk.
- **Phase 4—Adversarial Cybersecurity DT& E.** During this phase, an adversarial team tests the system's Cybersecurity and resilience using a mission context and in a cyber-contested operating environment using realistic threat exploitation techniques to identify residual risk.
- **Phase 5—Cooperative Vulnerability and Penetration Assessment.** The purpose of this phase is to fully characterize the Cybersecurity and resilience status of a system in a fully operational context and provide reconnaissance of the system in support of Adversarial Assessments.
- **Phase 6—Adversarial Assessment.** Phase 6 characterizes the operational mission effects to critical missions caused by threat-representative cyber activity against a unit trained and equipped with a system, as well as the effectiveness of defensive capabilities.

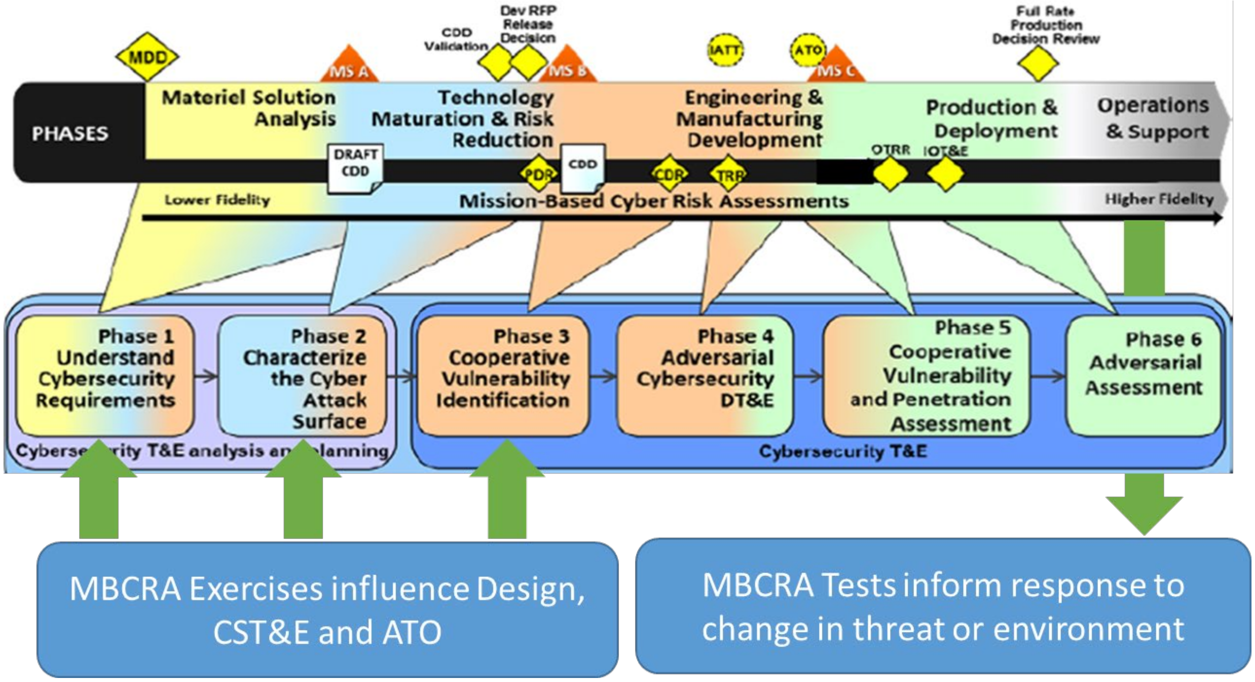

MDD
MS A
CDD Validation
Dev RFP Release Decision
MS B
IATT
ATO
MS C
Full Rate Production Decision Review
PHASES
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
DRAFT CDD
PDR
CDD
CDR
TRR
OTRR
IOT&E
Lower Fidelity
Mission-Based Cyber Risk Assessments
Higher Fidelity
Phase 1 Understand Cybersecurity Requirements
Phase 2 Characterize the Cyber Attack Surface
Phase 3 Cooperative Vulnerability Identification
Phase 4 Adversarial Cybersecurity DT&E
Phase 5 Cooperative Vulnerability and Penetration Assessment
Phase 6 Adversarial Assessment
Cybersecurity T&E analysis and planning
Cybersecurity T&E
MBCRA Exercises influence Design, CST&E and ATO
MBCRA Tests inform response to change in threat or environment

Figure F-5 MBCRA in the Cyber T&E Process

7.0. Phase 1 and 2: MBCRA

Figure F-5 depicts the MBCRA activities mapped against the CSTE phases aligned to the DoDI 5000.02 acquisition life cycle. A key feature of effective CSTE is early involvement of Cybersecurity testers in test analysis and planning. Each CSTE phase includes analysis and planning activities for the subsequent phases, starting in Phase 1.

DoDI 5000.02, updated in 2020 with Enclosure 14, Cybersecurity in the Defense Acquisition System, outlines responsibilities the PM implements to safeguard acquisition systems from Cybersecurity-related risks throughout the system life cycle, one such safeguard is the MBCRA. This process identifies, estimates, assesses, and prioritizes risks based on impacts to operational missions resulting from cyber effects on the system employed.

The systems engineering activities accomplished throughout the execution of the SSE Cyber workflow process generate much of the data needed for further analysis during Test and Evaluation (T&E), specifically for the MBCRAs. According to DOT&E policy[54], MBCRAs are mandatory for Phases 1 through 4 for DT&E (Table A-2), and Phase 5 and 6 (Table A-3) for OT&E. F-1 shows the alignment between the SSE Cyber Workflow Process and **MBCRA**s. The boxes outlined in red indicate where data/information is developed which would provide inputs/updates to a MBCRA.

> **NOTE:** Tailoring the Cybersecurity T&E phases is discouraged under the following conditions:
>
> - New architecture (numerous new interfaces)
> - Significant addition of key terrain items to a system architecture or system (typically when adding a new capability/large upgrades)
> - Significant change in intended operational environment
> - Significant changes in supply chain

For ACAT 2 and below programs, usually Agile-based products or services, conducting the MBCRA as early as Phase 1 through 3 for multiple capability releases may help to identify mission capability vulnerabilities prior to CTT.

Figure F-6 displays the MBCRA-related SSE Cyber Workflow Sub-Processes within the green box overlays. More guidance on the MBCRA can be found in the DoD Cybersecurity Test and Evaluation Guidebook. The recommended methodology for the MBCRA is the United States Air Force, "**Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook**".

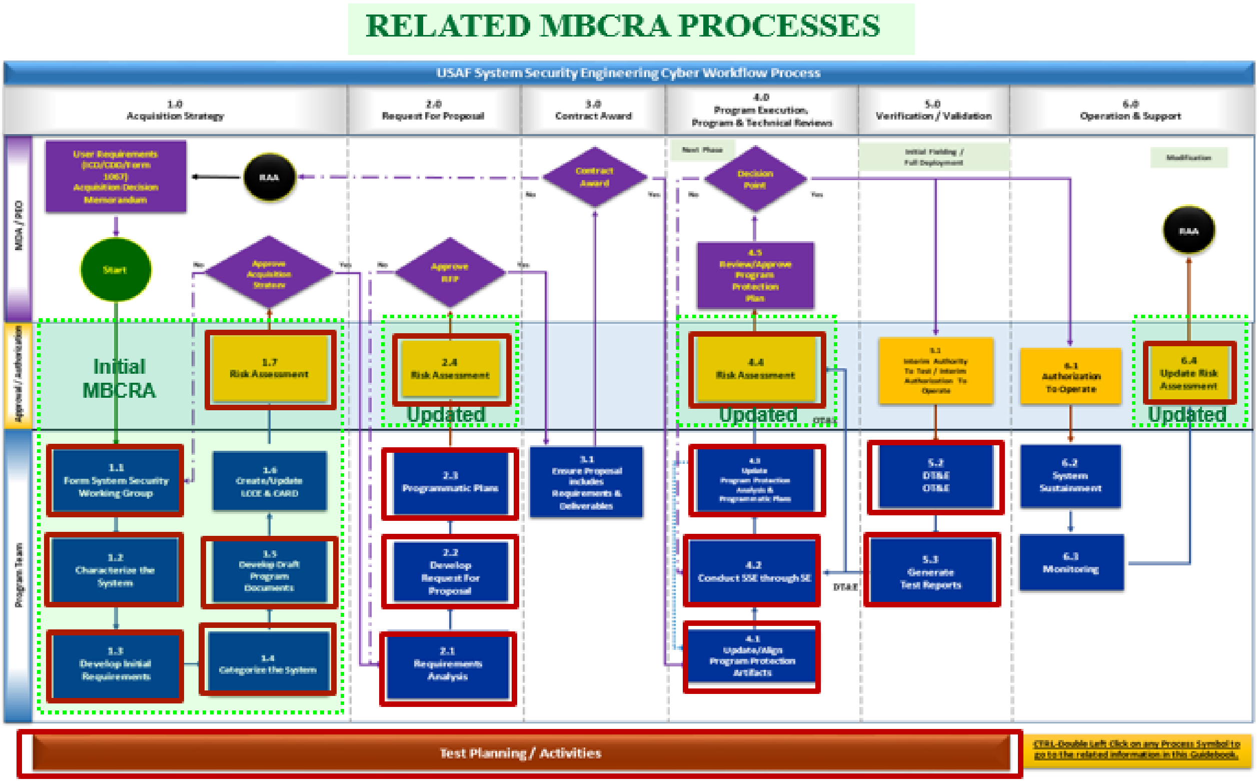

RELATED MBCRA PROCESSES
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
RAA
Start
Approve Acquisition Strategy
No
Yes
Approve RFP
Contract Award
Next Phase
Decision Point
Initial Fielding / Full Deployment
Modification
4.5 Review/Approve Program Protection Plan
Initial MBCRA
1.7 Risk Assessment
2.4 Risk Assessment
Updated
4.4 Risk Assessment
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
DT&E
1.1 Form System Security Working Group
1.6 Create/Update LCCE & CARD
1.2 Characterize the System
1.5 Develop Draft Program Documents
1.3 Develop Initial Requirements
1.4 Categorize the System
2.3 Programmatic Plans
2.2 Develop Request For Proposal
2.1 Requirements Analysis
3.1 Ensure Proposal includes Requirements & Deliverables
4.3 Update Program Protection Analysis & Programmatic Plans
4.2 Conduct SSE through SE
4.1 Update/Align Program Protection Artifacts
5.2 DT&E OT&E
5.3 Generate Test Reports
6.2 System Sustainment
6.3 Monitoring
Test Planning / Activities
CTRL-Double Left Click on any Process Symbol to go to the related information in this Guidebook.

Figure F-6 USAF SSE Cyber Workflow Process and Test and Evaluation

7.1 Phase 3: Cooperative Vulnerability Identification

Explicitly called out in Section 4.0 Work Breakdown Structure, items 4.2.8 and 5.2.2.1.

7.2 Phase 4: Adversarial Cybersecurity DT& E

Explicitly called out in Section 4.0 Work Breakdown Structure, item 5.2.2.2.

7.3 Phase 5: Cooperative Vulnerability and Penetration Assessment

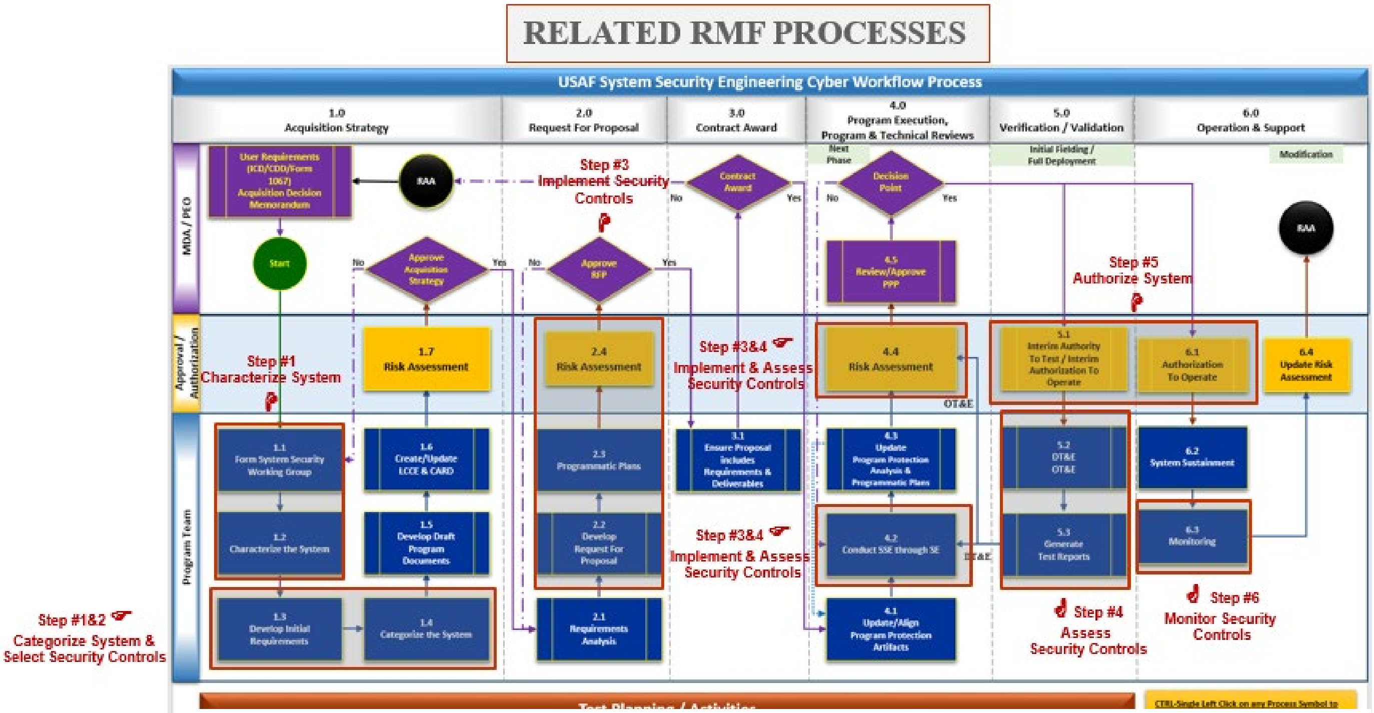
Explicitly called out in Section 4.0 Work Breakdown Structure, items 5.2.3 and 5.2.3.1.

7.4 Phase 6: Adversarial Assessment

Explicitly called out in Section 4.0 Work Breakdown Structure, items 5.2.3 and 5.2.3.2.

8.0. NIST RMF and the SSEG Workflow Processes

By executing the SSE Cyber Workflow Process, a significant amount of data required to support the RMF will be developed. Figure F-7 illustrates the RMF workflow process. Figure F-7, the grey box overlays illustrate the overarching areas the SSE Cyber Workflow Process supports/generate data for RMF.



RELATED RMF PROCESSES
USAF System Security Engineering Cyber Workflow Process
1.0 Acquisition Strategy
2.0 Request For Proposal
3.0 Contract Award
4.0 Program Execution, Program & Technical Reviews
5.0 Verification / Validation
6.0 Operation & Support
MDA / PEO
Approval / Authorization
Program Team
User Requirements (ICD/CDD/Form 1067) Acquisition Decision Memorandum
RAA
Start
Approve Acquisition Strategy
No
Yes
Approve RFP
Contract Award
Next Phase
Decision Point
Initial Fielding / Full Deployment
Modification
4.5 Review/Approve PPP
1.7 Risk Assessment
2.4 Risk Assessment
4.4 Risk Assessment
5.1 Interim Authority To Test / Interim Authorization To Operate
6.1 Authorization To Operate
6.4 Update Risk Assessment
OT&E
1.1 Form System Security Working Group
1.2 Characterize the System
1.3 Develop Initial Requirements
1.4 Categorize the System
1.5 Develop Draft Program Documents
1.6 Create/Update LCCE & CARD
2.1 Requirements Analysis
2.2 Develop Request For Proposal
2.3 Programmatic Plans
3.1 Ensure Proposal includes Requirements & Deliverables
4.1 Update/Align Program Protection Artifacts
4.2 Conduct SSE through SE
4.3 Update Program Protection Analysis & Programmatic Plans
5.2 OT&E OT&E
5.3 Generate Test Reports
6.2 System Sustainment
6.3 Monitoring
Step #1 Characterize System
Step #1&2 Categorize System & Select Security Controls
Step #3 Implement Security Controls
Step #3&4 Implement & Assess Security Controls
Step #3&4 Implement & Assess Security Controls
Step #4 Assess Security Controls
Step #5 Authorize System
Step #6 Monitor Security Controls
Test Planning / Activities
CTRL-Single Left Click on any Process Symbol to

Figure F-7 RMF Workflow Process

[54] Director Operational Test and Evaluation (DOT&E) Memo, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," 3 April 2018

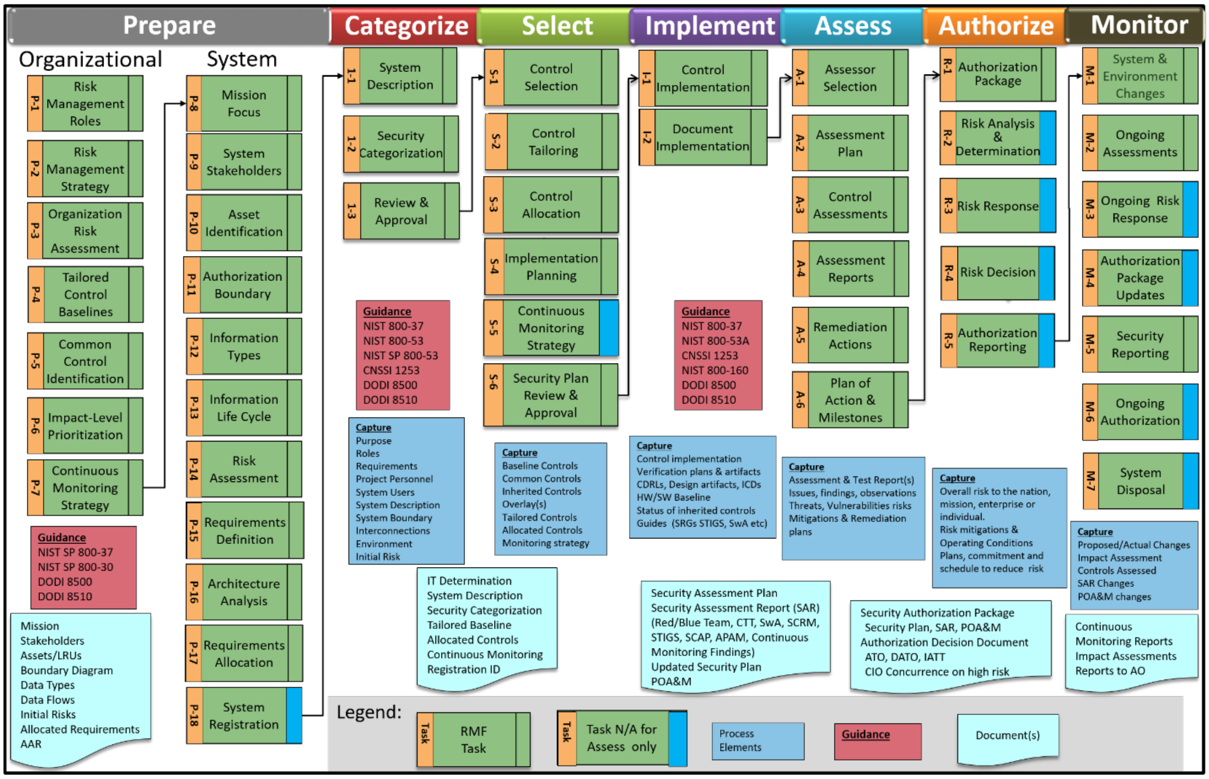


Figure F-8 USAF SSE Cyber Workflow Process

A more detailed mapping of the NIST standard RMF workflow steps in Figure F-8 is provided by Table F-2, and as controlled by Table F-1[55] forbidding certain working relationships as delineated by OUSD.

Table F-1 Allowable Working Relationships for RMF Team Members

Unallowable Relationships Among RMF Team Members
Authorizing Official (AO) cannot be or report to the Program Manager/System Manager (PM/SM), or Program Executive Officer (PEO)
Security Controls Assessor (SCA) cannot be or report to the PM/SM, or PEO
User Representatives cannot be or report to the PM/SM

[55] “Risk Management Framework (RMF) Knowledge Service (KS)”, **https://rmfks.osd.mil/rmf/Pages/default.aspx**

Table F-1 Trace between RMF Steps & SSECG WBS Steps

NIST SP800-37 r2.0													
RMF Tasks	**Expected Outcomes**	**SSECG WBS Task/Sub-Task (Table 4-1)**											
RMF: Prepare													
P-1	Identify and assign individuals to specific roles associated with security and privacy risk management.	**1.1.1**											
P-2	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	**1.2.6.1.2**											
P-3	Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.	**1.7**	**5.1.2**	**5.2.1**	**5.2.2**	**5.2.2.1**	**5.2.3**	**5.2.3.1**	**5.2.3.2**	**6.3.2**	**6.3.3**		
P-4	Establish, document, and publish organizationally tailored control baselines and/or Cybersecurity Framework Profiles.	**1.4.2**	**5.1.1**	**5.2.2.1**	**6.3.1**								
P-5	Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.												
P-6	Prioritize organizational systems with the same impact level.												
P-7	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.												
P-8	Identify the missions, business functions, and mission/business processes that the system is intended to support.	**1.2.1**	**1.2.3**	**1.2.4**	**1.2.6**	**1.2.6.1.1**	**1.2.6.3.2**	**1.2.6.3.3**	**1.2.9.5**	**1.7.4.1**	**5.2.3.2**		
P-9	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	**1.2.1**											
P-10	Identify assets that require protection.	**1.2.5**	**1.2.10**	**1.3.1**	**1.3.2**	**1.5.2**	**2.1**	**4.1.2**	**4.3**	**4.3.2**	**4.3.3**	**4.3.4**	**6.3.5**
P-11	Determine the authorization boundary of the system.	**1.2.4**											

NIST SP800-37 r2.0													
RMF Tasks	**Expected Outcomes**	**SSECG WBS Task/Sub-Task (Table 4-1)**											
P-12	Identify the types of information to be processed, stored, and transmitted by the system.	**1.2.5**	**1.4.1**	**1.5.1**	**4.1.2**	**4.3.3**	**4.3.4**	**6.3.6**					
P-13	Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.	**4.2.7**											
P-14	Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	**1.2.9**	**1.2.10**	**1.5.3**	**1.7.4**	**1.7.4.1**	**2.4**	**4.4**	**6.3.8**	**6.4**			
P-15	Define the security and privacy requirements for the system and the environment of operation.	**1.2.11**	**1.3.2**	**1.4.1**	**1.4.3**	**1.7.5**	**4.1.2**	**4.1.3**	**4.3.2**	**6.2**	**6.3.1**	**6.3.9**	
P-16	Determine the placement of the system within the enterprise architecture.	**4.2.2**											
P-17	Allocate security and privacy requirements to the system and to the environment of operation.	**1.4.3**	**4.1.3**	**4.2.6**	**5.2.3.1**	**6.2**							
P-18	Register the system with organizational program or management offices.	**5.1.2**	**6.1**										
RMF: Categorize													
C-1	Document the characteristics of the system.	**1.2.2**	**2.1**	**4.2.3**									
C-2	Categorize the system and document the security categorization results.	**1.2.11**	**1.4.2**										
C-3	Review and approve the security categorization results and decision.	**1.4.3**											
RMF: Select													
S-1	Select the controls for the system and the environment of operation.	**1.4.2**											
S-2	Tailor the controls selected for the system and the environment of operation.	**1.3**	**4.2**										
S-3	Allocate security and privacy controls to the system and to the environment of operation.	**1.3**	**4.2**										
S-4	Document the controls for the system and environment of operation in security and privacy plans.	**6.2**											

NIST SP800-37 r2.0

RMF Tasks	Expected Outcomes	SSECG WBS Task/Sub-Task (Table 4-1)											
S-5	Develop and implement a system level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.	6.2											
S-6	Review and approve the security and privacy plans for the system and the environment of operation.	1.1.3	4.3	4.5	5.1.1								
RMF: Implement													
I-1	Implement the controls in the security and privacy plans.	4.2											
I-2	Document changes to planned control implementations based on the “as-implemented” state of controls.	1.3	4.2										
RMF: Assess													
A-1	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	1.1.1	5.1.1										
A-2	Develop, review, and approve plans to assess implemented controls.	1.1.1											
A-3	Assess the controls in accordance with the assessment procedures described in assessment plans.	5.2.2	5.2.3										
A-4	Prepare the assessment reports documenting the findings and recommendations from the control assessments.	5.2.2	5.2.2.1	5.2.2.2	5.2.3	5.2.3.1	5.2.3.2	5.3	6.3.2	6.3.8			
A-5	Conduct initial remediation actions on the controls and reassess remediated controls.	1.2.10.1	4.3.1	5.1.2									
A-6	Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.	4.3.1	5.1.2										
RMF: Authorize													
R-1	Assemble the authorization package and submit the package to the authorizing official for an authorization decision.	1.1.1	5.1.2										

NIST SP800-37 r2.0													
RMF Tasks	**Expected Outcomes**	**SSECG WBS Task/Sub-Task (Table 4-1)**											
R-2	Analyze and determine the risk from the operation or use of the system or the provision of common controls.	**1.2.6.1.2**	**1.2.9.4**	**4.3**	**4.3.3**	**5.1.2**							
R-3	Identify and implement a preferred course of action in response to the risk determined.	**5.1.2**											
R-4	Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	**5.1.2**	**6.1**										
R-5	Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.	**5.1**	**5.2.3.1**	**5.2.3.2**	**6.1**								
RMF: Monitor													
M-1	Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.	**6.2**											
M-2	Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.	**6.3.1**	**6.3.8**	**6.3.9**									
M-3	Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.	**1.1.4**	**1.2.10**	**1.2.10.1**	**1.5.1**	**1.7.5**	**1.7.5**	**6.3.2**					
M-4	Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.	**6.3.2**	**6.4**										
M-5	Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.	**6.3.3**	**6.3.8**										
M-6	Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.	**6.3.9**	**6.4**										

NIST SP800-37 r2.0													
RMF Tasks	Expected Outcomes	SSECG WBS Task/Sub-Task (Table 4-1)											
M-7	Implement a system disposal strategy and execute required actions when a system is removed from operation.	6.3.4											

APPENDIX G

DEFINITIONS

Acquisition: The conceptualization, initiation, design, development, test, contracting, production, fielding, deployment, sustainment, and disposal of a directed and funded effort that provides a new, improved, or continued materiel, weapon, information system, logistics support, or service capability in response to an approved need (AFPD 63-1).

Acquisition Security Database (ASDB): The DoD horizontal protection database providing online storage, retrieval, and tracking of CPI and supporting program protection documents to facilitate comparative analysis of defense systems' technology and align CPI protection activities across the DoD (DoDI 5200.39).

Additional Performance Attributes (APA): Performance Attributes of a system not important enough to be a KPP or KSA. An APA must be measurable, testable, and support efficient and effective V&V by T&E. APAs are identified by their Sponsor and should be kept to a minimum. Changes to the APA are delegated by the DoD requirements approving authority to their Sponsor, unless retained in a DoD-level document validation memorandum.

Advanced Persistent Threat (APT): An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltration information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives (Refs. CNSSI No. 4009, NIST SP800-39).

Adversarial Assessment (AA): Gauges the ability of a system to support its mission(s) while withstanding validated and representative cyber threat activity. Evaluates the ability to protect the system/data, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity; these capabilities are collectively referred to as PDRR – Protect, Detect, React, and Restore (DOT&E TEMP Guidebook).

Adversary: Individual, group, organization, or Government that conducts or has the intent to conduct detrimental activities (CNSSI No. 4009, NIST SP800-39).

Air Force Federal Acquisition Regulation Supplement (AFFARS): The AFFARS establishes uniform policies and procedures for the AF implementing and supplementing the FAR, the DFARS, and other DoD publications concerning contracting.

Anti-Tamper (AT): Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering DoDD 5200.47E).

Anti-Tamper Executive Agent (ATEA): The DoD ATEA, consisting of the Update this to USD (R&E), USD (I&S) and USD (A&S) are located within the Secretary of the Air Force, Acquisition and Logistics (SAF-AQL) organization. SAF-AQL establishes AT guidance, conducts training, and conducts analysis in coordination with the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (A&S) (DoDI 5200.39, Headquarters AF Mission Directive 1-10) and DoDD 5200.47E.

Applicable Systems:

- National security systems as defined by Section 3552 of title 44, United States Code (U.S.C.) (Reference (l)). Although DoD's Non-classified Internet Protocol Router Network (NIPRNet) and its enclaves are considered national security systems in accordance with CJCS Instruction 6211.02D (Reference (m)), they are exempted from this instruction due to the need to prioritize use of limited TSN enterprise capabilities unless paragraph 2.b.(2) or 2.b.(3) applies;

- Any DoD system with a high impact level for any of the three security objectives (confidentiality, integrity, and availability) in accordance with the system categorization procedures in DoDI 8510.01 (Reference (n)); or

- Other DoD information systems that the DoD Component's acquisition executive or chief information officer, or designee, determines are critical to the direct fulfillment of military or intelligence missions, which may include some connections to or enclaves of NIPRNet and some industrial control systems. (DoDI 5200.44)

Asset: A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations. (DoDD 3020.40).

Assurance: Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy (CNSSI No. 4009).

Assurance Case: Means representation of a claim or claims, and support for these claims (ISO/IEC 15026-1:2013). A Software Assurance Case includes (software assurance) claims and evidence that support those (software assurance) claims (CNSSI No. 4009).

Capability: The ability to complete a task or execute a course of action under specified conditions and level of performance. (CJCSI 5123.01H).

Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Component Acquisition Executive (CAE): The single official within a DoD component that is responsible for all acquisition functions within that component. This includes Secretaries of the Military Departments or Heads of Agencies with the power of regulation.

Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises

Controlled Technical Information (CTI): Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions (DFARS 252.204-7012).

Cooperative Vulnerability and Penetration Assessments (CVPA): An overt and cooperative examination of the system to identify all significant cyber vulnerabilities and the level of capability required to exploit those vulnerabilities (DOT&E TEMP Guidebook).

Counterfeit: An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source, and has been misrepresented to be an authorized item of the legally authorized source (18 U.S.C. § 2320).

Counterfeit Materiel: An unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be authentic, unmodified material from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer (DFARS Clause 252.246–7007).

Countermeasures: The employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. (DoDI 5200.39) Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken (CNSSI No. 4009).

Critical Component (CC): A component which is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system (DoDI 5200.44).

Critical Intelligencer Parameter: Represent key performance thresholds of foreign threat systems, which, if exceeded, could compromise the mission effectiveness of the system in design, develop, test and evaluate IMD-dependent sensors, algorithms, systems, processes and interfaces.

Critical Program Information (CPI): United States (U.S.) capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment (DoDI 5200.39).
Critical Space Vehicle Functions (Critical Functions): The functions of the vehicle that the operator must maintain to ensure intended operations, positive control, and retention of custody. The failure or compromise of critical space vehicle functions could result in the space vehicle not responding to authorized commands, loss of critical capability, or responding to unauthorized commands.

Criticality: A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function (CNSSI No. 4009, NIST SP800-60).

Criticality Analysis (CA): An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s) (DoDI 5200.44).

Criticality Level: Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level (CNSSI No. 4009).

Cyber (adj.): Of or pertaining to the cyberspace environment, capabilities, plans, or operations (AFPD 17-2).**Cyber-Physical System (CPS):** Are smart systems that include engineered interacting networks of physical and computational components.

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 (Refs. NSPD-54/ HSPD-23, CNSSI No. 4009).

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12R).

Cyber Attack Surface: The system's use of COTS, GOTS, planned system interfaces, protocols, and operating environment that represents a collection of vectors threats may use to access, disrupt, destroy, or deny use of a network service, information system, or other forms of computer based system. Vectors include, but are not limited to: hardware flaws, firmware, communications links (local area network, wide area network, wireless, etc.), physical interfaces (Universal Serial Bus, Firewire), software (operating system applications, basic in-put/output system), and open communication ports and communication protocols (HTTP, FTP, PPP) (DoD PM's Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Lifecycle).

Cyber Incident: Actions taken using an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (CNSSI No. 4009). In this guidebook, "cyber incident" is used interchangeably with "cyber event".
Cyber Resiliency: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources (NIST SP800-160, Vol. 2).

The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. (NIST SP800-34).

Cyberspace Defense: Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate (DoDI 8500.01).

Cyber Survivability: The ability of a system to prevent, mitigate and recover from cyber-attacks. (paraphrased from the Manual for the Operation of the JCIDS). Within this SSECG, Cyber Survivability is used as an overarching term to include both Cybersecurity and Cyber Resiliency.

Cyber Survivability Risk Category (CSRC): Identifies appropriate strength of implementation levels (1-4) for Cyber Survivability (CJCS CSEIG).

Defense Federal Acquisition Regulation Supplement (DFARS): The DoD supplement to the FAR system. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures.
http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Defensive Cyberspace Operations (DCO): Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems (JP 3-12R).

De-Identification: any process of removing the association between a set of identifying data and the data subject.

Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P): A Combatant Commander's strategic simulation of doctrine, organization, training, materiel, leadership and education, personnel, and facilities required to accomplish a mission.

Embedded Information Technology: Computer resources, both hardware and software, which are an integral part of a space, weapon, and weapon system (DoDI 5000.82).

Event: An observable occurrence in an information system or network (CNSSI No. 4009). Within this SSECG, "cyber event" is used interchangeably with "cyber incident".

Federal Acquisition Regulation (FAR): The FAR System governs the acquisition process by which the Government purchases (acquires) goods and services. The process consists of three phases: (1) need recognition and acquisition planning, (2) contract formation, and (3) contract administration.

https://acquisition.gov/far/

Firmware: Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs (NIST SP800-171, Rev. 1).
Fuzz Testing: A software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions, such as crashes, failing built-in code assertions, or potential memory leaks (ISO/IEC/IEEE 29119-4:2015).

Initial Concept Design Review (ICDR): Conducted before the Materiel Development Decision (MDD) where the initial concept baseline(s) will be established. The ICDR will be chaired by a USD(R&E) representative for joint missions and by the applicable Service representative for Service-specific missions.

Horizontal Protection: Application of a consistent level of protection to similar CPI associated with more than one Research, Development, Test, and Evaluation (RDT&E) program, including inherited CPI (DoDI 5200.39).

Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Industrial Control System: General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) (CNSSI 4009).

Infrastructure-as-Code (IaC): the management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as DevOps team uses for source code. Like the principle that the same source code generates the same binary, an IaC model generates the same environment every time it is applied. IaC is a key DevOps practice and is used in conjunction with continuous delivery.

Information and Communications Technology (ICT): Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT), as defined in Section 11101 of Title 40, U.S.C. (Reference (u)), rather, this term reflects the convergence of IT and communications (DoDI 5200.44).

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Information Technology: Any equipment, interconnected system, or interconnected subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, and services (including support services, and related resources). IT is equipment used by the DoD directly or is used by a contractor under a contract with the DoD that requires the use of that equipment. IT does not include any equipment acquired by a federal contractor incidental to a federal contract (40 U.S.C., Sec. 1401).

Information Systems: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C., Sec. 3502).

Infrastructure: The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of Government at all levels, and to society as a whole (DoDD 3020.40).

Inherited CPI: CPI that is owned and generated by one RDT&E program, subsystem, or project that is incorporated into and used by another RDT&E program (DoDI 5200.39).

Malicious Code: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (NIST SP800-171).

Measure of Effectiveness (MOE): A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (DoD JP 3-0).

Measure of Performance (MOP): A criterion used to assess friendly actions that is tied to measuring task accomplishment (DoD JP 3-0).

Mission: The task, together with the purpose, that clearly indicates the action to be taken and the reason thereby. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task (DoD JP 3-0).

Mission Assurance: A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the execution of DoD mission-essential functions in any operating environment or condition (DoDD 3020.40).

Mission-Based Cyber Risk Assessment: The process of identifying, estimating, assessing, and prioritizing risks based on impacts to DoD operational missions resulting from cyber effects on the system(s) being employed (DoD Cybersecurity Test and Evaluation Guidebook).

Mission Critical Functions: Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed (DoDI 5200.44). Mission Critical Functions are analogous to Mission Essential Functions.

Mission Effects: Achieving reference missions and mission capabilities.

Mission Engineering (ME): The deliberate analyzing, planning, organizing and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects. (DAG Chapter 3/FY 2017 NDAA Section 855 Report to Congress).

Mission Essential Function: Mission Essential Functions. Mission Essential Functions (MEF) are those functions that organizations must continue throughout or resume rapidly after a disruption of normal activities and constitute the minimum vital and critical functions required to be provided and continued. MEFs are the basis for sustained continuity of operations and lack thereof constitutes mission failure (AFI 10-208). Mission Essential Functions are analogous to Mission Critical Functions.

Mission Focused Cyber Hardening (MFCH): The application of standards, processes, and procedures across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) spectrum to achieve operational resilience through Cyber Survivability such that weapons systems, supporting assets, and infrastructure can execute defense critical missions throughout their life cycle in a cyber-contested environment.

Mission Integration Management (MIM): The management, synchronization and coordination of concepts, activities, technologies, requirements, programs and budget plans to guide key decisions focused on the end-to-end mission. Department of Defense (DoD) Mission Engineering (ME) Guidebook, November 2020.

Mission Thread: A sequence of end-to-end activities and events beginning with an opportunity to detect a threat or element that ought to be attacked and ending with a commander’s assessment of damage after an attack (Software Engineering Institute).

National Security System: Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency:
"(i) the function, operation, or use of which—

> *(I) involves intelligence activities;*
>
> *(II) involves cryptologic activities related to national security;*
>
> *(III) involves command and control of military forces;*
>
> *(IV) involves equipment that is an integral part of a weapon or weapons system; or*
>
> *(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or*
>
> *(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.*

(B) Subparagraph (A) (i) (V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (44 U.S.C. SEC 3542)"

Operational Resilience: 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 (DoDI 8500.01).

Organic CPI: Unique CPI that is owned and generated by an RDT&E program (DoDI 5200.39).

Patch: A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component (ISO/IEC 19770-2).

Patch Management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs (CNSSI 4009).

Penetration Testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system (CNSSI No. 4009).

Plan of Action and Milestones (POA&M): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones (OMB Memorandum 02-01).

Platform Information Technology (PIT): Both hardware and software that are physically a 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 systems may be structured by physical proximity or by function, independent of location (DoDI 8500.01).

Positive Control: The assurance that a space vehicle will only execute commands transmitted by an authorized source and that those commands are executed in the proper order and at the intended time.

Program Protection (PP): The integrating process for mitigating and managing risks to advanced technology and mission critical system functionality from foreign collection, design vulnerability, or supply chain exploitation/insertion, battlefield loss, and unauthorized or inadvertent disclosure throughout the acquisition life cycle (DoDI 5000.83).

Program Protection Plan (PPP): Describes the program's mission critical functions, as well as, its CPI and critical components providing, protecting, or having unrestricted access to mission critical functions. The PPP documents the threats to, and vulnerabilities of its CPI and critical components; describes the program's risk management approach; details the selection, application, and estimated cost of countermeasures to mitigate associated risks; and describes all foreign involvement.

> (**NOTE:** The Program Protection Implementation Plan (PPIP) is the contractor's instantiation of the PPP.) (AFPAM 63-113).

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Program Protection Planning: A comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment, and facilities (AFPAM 63-113).

Provisional Authorization: A pre-acquisition type of Risk Management Framework Information System Authorization used by DoD and FedRAMP to pre-qualify Commercial CSOs to host Federal Government and/or DoD information and information systems. PAs are to be used by Federal and DoD Cloud Mission Owners during source selection and subsequent system authorization under RMF.

Public Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Resilience: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Refs. White House Office of Management and Budget Circular No. A-130 and CNSSI No. 4009).

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs, and (2) the likelihood of occurrence (CNSSI No. 4009).

Risk Management: A process by which decision makers accept, reduce, or offset risk, and subsequently make decisions that weigh overall risk against mission benefits. Risk management is composed of risk assessment and risk response (DoDD 3020.40).

Risk Management Framework (RMF): Provides a disciplined and structured process that combines information system security and risk management activities into the system development life cycle and authorizes their use within DoD. The RMF has six steps: categorize system; select security controls; implement security controls; assess security controls; authorize system; and monitor security controls (DoDI 8500.01).

Safety Critical Function: A function whose failure to operate or incorrect operation will directly result in a mishap of either Catastrophic or Critical severity. (AC-17-01/MIL-STD-882)

Security Categorization: The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSSI No. 1253 for national security systems and in FIPS 199 for other than national security systems (CNSSI No. 4009).

Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation (CNSSI No. 4009).

Security Control: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (CNSSI No. 4009).

Security Control Assessor (SCA): The individual, group, or organization responsible for conducting a security control assessment (CNSSI No. 4009).

Security Requirements: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted (CNSSI No. 4009).

Security Requirements Guide (SRG): Compilation of control correlation identifiers (CCIs) grouped in more applicable, specific technology areas at various levels of technology and product specificity. Contains all requirements that have been flagged as applicable from the parent level regardless if they are selected on a Department of Defense (DoD) baseline or not (DoDI 8500.01).

Security Technical Implementation Guide (STIG): Based on DoD policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline (DoDI 8500.01).

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 life cycle (Refs. DoDI 5200.44 and AFPAM 63-113).

Software Assurance Techniques: Processes and procedures utilized to verify both the expected functional and security performance of software. Example techniques can include but are not limited to static and dynamic code analysis and testing, resilient software design implementations, secure and consistent coding practices, system security and functional testing, system and software integrity via supply chain risk management, regression testing for patching, reliability, performance, and software disposal. **http://cwe.mitre.org**

Space System: A combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service. A space system typically has three segments: a ground control network, a space vehicle, and a User or mission network. These systems include Government national security space systems, Government civil space systems, and private space systems.

Space Vehicle: The portion of a space system that operates in space. Examples include satellites, space stations, launch vehicles, launch vehicle upper stage components, and spacecraft.

Supply Chain: The linked activities associated with providing materiel to end Users for consumption. Those activities include supply activities (such as organic and commercial ICPs and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters) (DoDI 4140.01).

Supply Chain Risk: The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (DoDI 5200.44).

Supply Chain Attack: Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products), or services at any point during the life cycle (CNSSI No. 4009).

Supply Chain Risk Management (SCRM): The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system. DoD SCRM encompasses all sub-sets of SCRM, such as Cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain (DoDI 4140.01 *DoD Supply Chain Materiel Management Policy*).

Survivability: All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy (JP 3-34).

The ability of a system to minimize the impact of a finite- duration disturbance on value delivery (i.e., stakeholder benefit at cost), achieved through the reduction of the likelihood or magnitude of a disturbance; the satisfaction of a minimally acceptable level of value delivery during and after a disturbance; and/or a timely recovery (NIST SP800-160, Vol. 2).

System Assurance: The justified measures of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle (DoDI 5200.39).

System Security: Protection of systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized Users, including those measures necessary to detect, document, and counter such threats (CNSSI 4009).

Systems Engineering (SE): 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 (DoDI 5000.88).

Systems Security Engineering (SSE): An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities (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 No. 4009).

Threat Assessment: Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat (CNSSI No. 4009).

Threat Event: An event or situation that has the potential for causing undesirable consequences or impact (NIST SP800-30 r1.0).

Threat Source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability (CNSSI No. 4009).

Trusted Systems and Networks (TSN): A DoD strategy and set of concepts to minimize the risk that DoD's warfighting capability will be impaired due to vulnerabilities in system design, sabotage, or subversion of a system's critical functions or critical components by foreign intelligence, terrorists, or other hostile elements. TSN levies requirements for Supply Chain Risk Management, hardware assurance, software assurance, and trusted foundry (Refs. DoDI 5200.44, AFPAM 63-113).

Validated Online Lifecycle Threat (VOLT): Replacement document for the STAR circa FY17 (Ref. DoDI 5200.02). VOLT Report forms are located at: **https://intellipedia.intelink.sgov.gov/wiki/TLA-3** .

Vulnerability: Weakness in system, system security procedures, internal controls, or implementation that could be exploited by a threat source (Ref. CNSSI No. 4009).

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 (Ref. CNSSI No. 4009).

Weapon System: A combination of elements that function together to produce the capabilities required for fulfilling a mission need, including hardware, equipment, software. Excluding supporting infrastructure and IT systems (Paraphrased from AFPAM 63-128). A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency (Ref: Joint Pub 1-02).

APPENDIX H

ACRONYMS

Acronym	Definition
AA	Adversarial Assessment
AAF	Adaptive Acquisition Framework
AoA	Analysis of Alternatives
A&AS	Advisory & Assistant Services
ACAT	Acquisition Category
ACD	Adversarial Cyber Developmental Test & Evaluation
ACE	Acquisition Center of Excellence
ACL	Access Control List
ACQ	Acquisition
ACTA	Adversary Cyber Threat Analysis
A/D	Analog to Digital
ADM	Acquisition Decision Memorandum
AFFARS	Air Force Federal Acquisition Requisition Supplement
AFI	Air Force Instruction
AFLCMC	Air Force Life Cycle Management Center
AFMAN	Air Force Manual
AFNWC	Air Force Nuclear Weapons Center
AFOSI	Air Force Office of Special Investigations
AFPAM	Air Force Pamphlet
AFPD	Air Force Policy Directive
AFRL	Air Force Research Lab
AFTE	Air Force Test & Evaluation
AIG	Acquisition Intelligence Guide
AO	Authorizing Official
AoA	Analysis of Alternatives
AP	Acquisition Plan
APA	Additional Performance Attributes
APA	Attack Path Analysis
APAR	Attack Path Analysis Report
APE	Attack Path Exercise
APTV	Attack Path Analysis Template
APV	Attack Path Vignettes
ARRT	Acquisition Requirements Roadmap Tool
ARTCP	Adaptive Rate Transmission Control Protocol
AS	Acquisition Strategy
ASAC	Application of Software Assurance Countermeasures
ASDB	Acquisition Security Database
ASIC	Application-Specific Integrated Circuit
ASICs	Application-Specific Integrated Circuits

Acronym	Definition
ASP	Acquisition Strategy Panel
ASPM	Acquisition Security Program Manager
ASR	Alternative Systems Review
AT	Anti-Tamper
ATC	Approval to Connect
ATEA	Anti-Tamper Executive Agent
ATEP	Anti-Tamper Evaluation Plan
ATER	Anti-Tamper Evaluation Report
ATET	Anti-Tamper Evaluation Team
ATO	Authorization to Operate
ATP	Anti-Tamper Plan
AV	All Viewpoint
BAA	Broad Agency Announcement
BCAC	Business Capability Acquisition Cycle
BOE	Body of Evidence
BOM	Bill of Materials
C2	Command & Control
CA	Critical Analysis
CAC	Common Access Card
CAE	Component Acquisition Executive
CAIG	CPI Assessment & Identification Code
CAPEC	Common Attack Pattern Enumeration & Classification
CARD	Cost Analysis Requirements Document
CC	Critical Components
CCA	Clinger-Cohen Act
CCE	Common Computing Environment
CCP	Common Controls Provider
CDD	Capability Development Document
CDI	Covered Defense Information
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDS	Cross Domain Solution
CDT	Chief Developmental Tester
CE	Chief Engineer
CI	Configuration Item
CI	Counterintelligence
CICA	Classified Information Compromise Assessment
CICC	Cyber Incident Coordination Cell
CIO	Chief Information Officer
CIP	Critical Intelligence Parameter
CISP	Counterintelligence Support Plan
CJA	Central Intelligence Agency
CLO	Counter Low Observable

Acronym	Definition
CJCSI	Chairman of the Joint Chiefs of Staff
CM	Configuration Management
CMMC	Cyber Maturity Model Certification
CMMI	Capability Maturity Model Integration
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CoC	Certificate of Conformance
CoC	Consequence of Compromise
Coffs	Consequence of Compromise Analysis
COI	Community of Interest
COMPUSEC	Computer Security
COMSEC	Communication Security
CONEMP	Concepts of Employment
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CPD	Capability Production Documents
CPI	Critical Program Information
CPM	Capability Portfolio Management
CPS	Cyber Physical System
CRA	Cyber Risk Assessment
CRM	Comment Resolution Matrix
CROWS	Cyber Resiliency Office for Weapon Systems
CSRP	Cyber Survivability Risk Posture
CR-TAC	Cyber Resiliency Technical Advisory Council
CRYPTO	Cryptographic
CS	Cybersecurity Strategy
CSA	Cyber Survivability Attributes
CSAR	Cyber Survivability Report
CSCI	Computer Software Configuration Item
CSE	Cyber Survivability Endorsement
CSEIG	Cyber Survivability Endorsement Implementation Guide
CSIP	Cybersecurity Implementation Plan
CSRC	Cyber Survivability Risk Category
CSRP	Cyber Survivability Risk Posture
CSSLP	Certified Secured Software Lifecycle Professional
CSSP	Cyber Security Service Providers
CSTE	Cyber Security Test & Evaluation
CST&E	Cybersecurity DT&E
CT	Critical Technologies
CTA	Capstone Threat Assessment
CTE	Chief Technology Element
CTES	Critical Technology Elements

Acronym	Definition
CTES	Cyber Test & Evaluation Strategy
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
CV	Capability Viewpoint
CVE	Common Vulnerabilities & Exposure
CVI	Cooperative Vulnerability Identification
CVPA	Collective Vulnerability & Penetration Assessment
CVRA	Critical Vulnerability Risk Assessment
CWBS	Contractor Work Breakdown Structure
CWE	Common Weakness Enumeration
CyWG	Cybersecurity Working Group
D/A	Digital to Analog
DAB	Defense Acquisition Board
DAE	Defense Acquisition Executive
DAF	Department of the Air Force
DAG	Defense Acquisition Guide
DAR	Damage Assessment Report
DASD(SE)	Deputy Assistant Secretary of Defense for System Engineering
DAU	Defense Acquisition University
DC3	Defense Cyber Crime Center
DCO	Defensive Cyberspace Operations
DCS	Direct Commercial Sales
DCS	Distributed Control System
DCSA	Defensive Counterintelligence and Security Agency
DD	Department of Defense
DEF	Defense Exportability Features
DFARS	Defense Federal Acquisition Regulation Supplement
DFARS	Defense Federal Acquisition Regulation System
DIA	Defense Intelligence Agency
DIA-CAP	DoD Information Assurance Certification Accreditation Process
DIA-TAC	Defense Intelligence Agency Threat Assessment Center
DID	Data Item Description
DISA	Defense Systems Information Systems
DITPR	Department of Defense Intelligence Technology Portfolio Registry
DMEA	Defense Microelectronics Agency
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoD CIO	Department of Defense Chief Information Officer
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DoDM	Department of Defense Manual
DOORS	Dynamic Object-Oriented Requirements System

Acronym	Definition
DOT&E	Director Operational Test & Evaluation
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy
DR	Deficiency Report
DSQ	Decision Support Questions
DSS	Defense Security Service
DSTL	Defense Science & Technology List
DT	Developmental Test
DT&E	Developmental Test & Evaluation
E3	Electromagnetic Environmental Effects
EA	Electronic Attack
EAP	Entry Access Points
EAR	Export Administration Regulations
EASA	European Union Aviation Safety Agency
ECR	Export Control Reform
ECU	End Cryptographic Unit
EDPU	Electrical Power Drive Unit
EI	Engineering Instruction
EITDR	Enterprise Information Technology Data Repository
ELA	Enterprise Licensing Agreement
eMASS	Enterprise Mission Assurance Support Service
EMD	Engineering, Manufacturing & Development Phase
EMS	Enterprise Master Schedule
EO/IR	Electro-Optical/Infrared
EP	Electronic Protection
ESI	Enterprise Software Initiative
ESLOC	Equivalent Source Lines of Code
ESOH	Environmental, Safety & Occupational Health
EXCOM	Executive Committee of the National Security Council
FAA	Federal Aviation Administration
FACE	Future Airborne Capability Environment
FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FDCCI	Federal Data Center Consolidation Initiative
FDD	Full Deployment Decision
FDO	Foreign Disclosure Officer
FDP	Firmware Development Plan
FFRDC	Federally Funded Research & Development Center
FIPS	Federal Information Processing Standards
FMEA	Failure Modes Effects & Analysis
FMS	Foreign Military Sales
FOC	Full Operational Capability
FOSS	Free & Open Source Software

Acronym	Definition
FOUO	For Official Use Only
FPGA	Field Programmable Gate Array
FRD	Functional Requirements Document
FQT	Factory Qualification Test
FRP	Full Rate Production
FRP/FD	Full Rate Production/Full Deployment
FSM	Firmware Support Manual
FTA	Fault Tree Analysis
FTA	Functional Thread Analysis
FW	Firmware
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GIDEP	Government-Industry Data Exchange Program
GOTS	Government off-the-shelf
HAF	Headquarters Air Force
HDP	Hardware Development Plan
HLO	High Level Objectives
HPG	Horizontal Protection Guidance
HPT	High Performance Team
HUMS	Health & Usage Monitoring Systems
HW	Hardware
HwA	Hardware Assurance
IA&E	International Acquisition & Exportability
IASRD	Information Assurance Requirements Document
IATT	Interim Authorization to Test
IAW	In Accordance With
IB	Implementation Baseline
IBR	Integrated Baseline Review
IC	Intelligence Community; International Cooperatives
IaC	Infrastructure-as-Code
IaaS	Infrastructure as a Service
ICD	Initial Capabilities Document
ICD	Interface Control Document
ICDR	Initial Concept Design Review
ICT	Information & Communications Technology
ID	Identification
IdAM	Identity & Access Management
IDD	Interface Design Document
IDS	Intrusion Detection System
IE	Information Enterprise
IEC	International Electro technical Commission
ILC	Integrated Life Cycle
IMP	Integrated Master Plan

Acronym	Definition
IMS	Integrated Master Schedule
INCOSE	International Council on Systems Engineering
INFOSEC	Information Security
IO	Information Operations
IOC	Initial Operational Capability
IOT&E	Initial Operational Test & Evaluation
IP	Information Protection
IP	Intellectual Property
IP	Internet Protocol
IPMR	Integrated Program Management Report
IPT	Integrated Product Team
IPv6	Internet Prototype Version 6
IR&D	Independent Research & Development
IRT	Incident Response Team
IS-CDD	Information Security Capability Development Document
IS-ICD	Information Security Initial Capabilities Document
ISO	Information Security Officer
ISP	Information Support Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITA	Integrated Threat Assessment
ITAR	International Traffic in Arms Regulation
ITCC	Information Technology Commodity Council
ITIPS	Information Technology Investment Portfolio System
ITRA	Independent Technical Risk Assessment
ITT	Integrated Test Team
IUID	Item Unique Identification
JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration Development System
JCS	Joint Chief of Staff
JDRS	Joint Deficiency Requirements System
JELA	Joint Enterprise Licensing Agreement
JFAC	Joint Federated Assurance Center
JIE	Joint Information Environment
JITC	Joint Inoperability & Test Command
JP	Joint Publication
KCMP	Key & Certificate Management Plan
KMI	Key Management Infrastructure
KMP	Key Management Plan
KPP	Key Performer Parameter
KS	Knowledge Service
KSA	Key System Attribute

Acronym	Definition
LBC	Logic Bearing Components
LCCE	Life Cycle Cost Estimate
LCRIT	Logistics Cyber Risk Identification Tool
LCRM	Life-Cycle Risk Management
LCSP	Life-Cycle Sustainment Plan
LDTO	Lead Developmental Test Organization
LE	Lead Engineer
LO	Low Observable
LOA	Line of Action
LOA	Letter of Agreement
LO/CLO	Low Observable / Counter Low Observable
LOR	Letter of Requirement
LRU	Line Replaceable Unit
LSE	Lead System Engineer
MAAP	Master Air Attack Plan
MAJCOM	Major Command
MAU	Modular Acquisition Unit
MBCRA	Mission Based Cyber Risk Assessment
MBSE/DE	Model Based Systems Engineering/Digital Engineering
MCF	Mission Critical Function
MFCH	Mission Focused Cyber Hardening
MCTL	Military Critical Technology List
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
ME	Mission Engineering
MGCH	Mission Focused Cyber Hardening
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MIM	Mission Integration Management
MOA	Memoranda of Agreement
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOU	Memoranda of Understanding
MOSA	Modular Open System Assessment
MRAP-C	Mission-based Risk Assessment Process for Cyber
MS	Milestone
MTA	Middle Tier for Acquisition
NAR	Non-Advocate Review
NASIC	National Air & Space Intelligence Center
NAVAIR	Naval Air Systems Command
NCES	Net-Centric Enterprise Services
NDA	Non-Disclosure Agreement
NDAA	National Defense Authorization Act

Acronym	Definition
NDI	Non-Developmental Item
NDIA	National Defense Industrial Association
NGO	Non-Governmental Organizations
NIAP	National Information Assurance Partnership
NIPRNet	Non-Classified Internet Protocol Router Network
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards & Technology
NRE	Non-Recurring Engineering
NSA	National Security Agency
NSS	National Security Systems
NSTIC	National Strategy for Trusted Identities in Cyberspace
NSTISSAM	National Security Telecommunications & Information Systems
OFP	Operational Flight Program
O&M	Operations & Maintenance
OMG	Object Management Group
OMS	Open Mission Systems
OPR	Office of Primary Responsibility
OPSEC	Operations Security
OS	Operating System
OSI	Office of Special Investigation
O&S	Operations & Support
O&S	Operations & Sustainment
OSD	Office of the Secretary of Defense
OT	Operational Test
OTA	Operational Test Agency
OTA	Other Transaction Agreements
OT&E	Operational Test & Evaluation
OTO	Operational Test Organization
OTRR	Operational Test Readiness Review
OTS	Off-The-Shelf
OV	Operational Viewpoint
OWASP	Open Web Application Security Project
PA	Provisional Authorization
PBA	Performance-Based Agreement
PCA	Physical Configuration Audit
PCMCIA	Personal Computer Memory Card International Association
PCO	Procuring Contracting Officer
P&D	Production & Deployment
PD	Production & Development
PDR	Preliminary Design Review
PEG	Program Execution Group
PEO	Program Executive Order

Acronym	Definition
PERSEC	Personnel Security
PIT	Platform Information Technology
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PLD	Programmable Logic Device
PM	Program Manager
PM/CE	Program Manager / Chief Engineer
PMR	Program Management Review
PNT	Positioning, Navigation & Timing
PO	Program Office
POA&M	Plan of Actions & Milestones
POC	Point of Contact
POE	Program Office Estimate
PP	Program Protection
PPBE	Planning, Programming, Budgeting & Execution
PPIP	Program Protection Implementation Plan
PPP	Program Protection Plan
PPS	Program Protection Survey
PQM	Production, Quality & Manufacturing
PR	Production Requirement
PROM	Programmable Read-Only Memory
PRR	Production Readiness Review
PSS	Product Support Strategy
PWS	Performance Work Statement
QEB	Quantum Enterprise Buy
R&D	Research & Development
RAM	Random Access Memory
RAM	Reliability, Availability & Maintainability
RDT&E	Research, Development, Test & Evaluation
RE	Reverse Engineering
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposal
RIO	Risk, Issue & Opportunity
R&M	Reliability & Maintainability
RMB	Risk Management Board
RMF	Risk Management Framework
RMIS	Risk Management Information System
RMP	Risk Management Plan
ROM	Read Only Memory
ROM	Rough Order of Magnitude
RSS	Replaced System Sustainment

Acronym	Definition
RTVM	Requirements Traceability Verification Matrix
RVM	Requirements Verification Matrix
RWG	Risk Working Group
SA	Situational Awareness
SA	Security Assistance
SACM	Structured Assurance Case Metamodel
SAE	Service Acquisition Executive
SAFAQ	Secretary of the Air Force, Acquisition
SAF/AQL	Secretary of the Air Force, Acquisition & Logistics
SAF/CN	Deputy Chief Information Officer of the Air Force
SAP	Security Assessment Plan
SAPF	Special Access Program Facility
SAR	Security Assessment Report
SAT	Site Acceptance Test
SCA	Security Control Assessor
SCA-V	Security Control Assessment Validation
SCADA	Supervisory Control & Data Acquisition
SCAP	Secure Content Automation Protocol
SCC	Single Chip Crypto
SCF	Safety Critical Function
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SCTM	Security Controls Traceability Matrix
SDD	Software Design Document
SDK	Software Development Kit
SDP	Software Development Plan
SE	Systems Engineering
SEAMLS	Software Enterprise Acquisition Management & Life Cycle Support
SEI	Software Engineering Institute
SEI&T	Systems Engineering, Integration & Test
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Plan
SETA	Systems Engineering & Technical Assistance
SETRs	Systems Engineering Technical Reviews
SF	Standard Form
SFR	System Functional Review
SHP	Security Handling Plan
SIL	Systems Integration Lab
SIPRNet	Secret Internet Protocol Router Network
SLOC	Source Lines of Code
SMC	Space & Missile Command Center

Acronym	Definition
SMC/IN	SMC Directorate of Intelligence
SME	Subject Matter Expert
SoO	Statement of Objectives
SoS	System of Systems
SOW	Statement of Work
SP	Security Plan
SP	Standard Process
SP	Special Publication
SPRS	Supplier Performance Risk System
SRD	System Requirements Document
SRG	System Requirements Guide
SRR	System Requirements Review
SRS	Software Requirements Specification
SRU	Systems Replaceable Unit
SS	Systems Specification
SS	Systems Survivability
SSE	Systems Security Engineering
SSDD	System Segment Design Document
SSEB	Source Selection Evaluation Board
SSECG	Systems Security Engineering Cyber Guidebook
SSS	Staff Summary Sheet
SSWG	System Security Working Group
STAR	System Threat Assessment Report
STIG	Security Technical Implementation Guide
STINFO	Scientific and Technical Information
STP	Software Test Plan
STPA	System Theoretic Process Analysis
STR	Software Test Report
SUT	System Under Test
SV	Systems Viewpoint
SVPP	Survivability & Vulnerability Program Plan
SVR	System Verification Review
SVT	Security Verification Test
SW	Software
SwA	Software Assurance
SWAMP	Software Acquisition Management Plan
SWG	Survivability Working Group
T&E	Test & Evaluation
TA/CP	Technology Assessment / Control Plan
TAC	Threat Assessment Center
TARA	Threat Assessment and Remediation Analysis
TBC	Transient Bleed Control
TD	Technology Development

Acronym	Definition
TDY	Temporary Duty
TDS	Technology Development Strategy
TEMP	Test & Evaluation Master Plan
TIG	Technical Implementation Guide
TLA	Top Level Architecture
TMRR	Technical Maturation & Risk Reduction
TO	Technical Order
TO	Task Order
TPI	Technical Performance Indicators
TPM	Technical Performance Measure
TRA	Technical Readiness Assessment
TRANSEC	Transmission Security
TRL	Technical Readiness Level
TRR	Test Readiness Review
TRR	Technical Readiness Review
TS	Top Secret
TSC	Tri-Service Committee
TSN	Trusted Systems & Networks
TSRD	Telecommunications Security Requirements Document
TTP	Tactic, Technique or Procedure
UCI	Universal Command & Control Interface
UJT	Universal Joint Tasks
UON	Component/Joint Urgent Operational Needs
URL	Uniform Resource Locator
US	United States
USAF	United States Air Force
USB	Universal Serial Bus
USC	United States Code
US-CERT	United States Computer Emergency Response Team
USCYBERCOM	United States Cyber Command
USD (A&S)	Under Secretary of Defense for Acquisition & Sustainment
USD (P)	Under Secretary of Defense for Policy
USD (R&E)	Under Secretary of Defense for Research and Engineering
USML	United States Munitions List
VHDL	Very-High-Speed-Integrated-Circuits Hardware Description Language
VOIP	Voice-Over-Internet-Protocol
VOLT	Validated Online Life Cycle Threat
V&V	Validation & Verification
WARM	Wartime Reserve Code
WBS	Work Breakdown Structure
WoA	Wheel of Access

APPENDIX I

REFERENCES

CDRL

DI-ADMN-81249	Conference Agenda
DI-ADMN-81250	Conference Minutes
DI-CMAN-80858B	Technical Report Study/Services (addressing overall System Configuration)
DI-EMCS-81683	TEMPEST Test Plan
DI-EMCS-81684	TEMPEST Test Evaluation Report
DI-IPSC-81427B	Software Development Plan (SDP)
DI-IPSC-81433	Software Requirements Specification (SRS)
DI-IPSC-81435	Software Design Description (SDD)
DI-IPSC-81439	Software Test Description (STD)
DI-IPSC-81441	Software Product Specification (SPS)
DI-IPSC-82250	Software Attack Surface Analysis Report
DI-MGMT-80934	Operations Security (OPSEC) Plan
DI-MGMT-81026	TEMPEST Control Plan
DI-MGMT-81453	Data Accession List (DAL)

CDRL (continued)

- DI-MGMT-81763 Customized Microelectronics Devices Source Protection Plan
- DI-MGMT-81808 Contractor Risk Management Plan
- DI-MGMT-81809 Contractor Risk Management Status Report
- DI-MISC-80508 Technical Report Study/Services (addressing Attack Path Analysis)
- DI-MISC-81688 Key and Certificate Management Plan (KCMP)
- DI-MISC-81832 Counterfeit Prevention Plan
- DI-MSSM-81750 Department Of Defense (DoD) Modeling and Simulation (M&S) Accreditation Plan
- DI-MSSM-81751 Department Of Defense (DoD) Modeling and Simulation (M&S) Verification and Validation (V&V) Plan
- DI-MSSM-81752 Department Of Defense (DoD) Modeling and Simulation (M&S) Verification and Validation (V&V) Report
- DI-MSSM-81753 Department Of Defense (DoD) Modeling and Simulation (M&S) Accreditation Report
- DI-QCIC-80125 Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report
- DI-QCIC-81891 Acceptance Test Report (ATR)
- DI-SAFT-80101 System Safety Hazard Analysis Report
- DI-SAFT-81626 System Safety Plan
- DI-SESS-81022D Technical Report Study/Services (addressing overall System Configuration)
- DI-SESS-81248 Interface Control Document
- DI-SESS-81343 Information Security (INFOSEC) Boundary Configuration Management Plan

CDRL (continued)

- DI-SESS-81495 Failure Modes, Effects, and Criticality Analysis Report (FMECA)
- DI-SESS-81770 System/Software Integration Laboratory (SIL) Development and Management Plan
- DI-SESS-81785A Systems Engineering Management Plan (SEMP)
- RCM-FMEA DI-SESS-80980A Technical Report Study/Services (addressing FMEA)

Forms & Templates

- AF Form 1067, “Modification Proposal”, USAF, 1 November 1999
- DD Form 254, Department of Defense Contract Security Classification Specification (Instructions), USD (I&S), 29 January 2021

Guidance

- Acquisition Intelligence Guidebook (AIG), AFMC
- "Anti-Tamper (AT) Security Classification Guide", 30 July 2020 (U//FOUO)[56]
- "Best Practices Guide for Department of Defense Cloud Mission Owners", v1.0, 30 July 2015.
- "CPI Assessment and Identification Guide (CAIG)", v. 1.0, NDIA, 2 Aug 2019 (FOUO)
- "CPI/LO/CLO Workbook Template 1.0 - Classified HPG and 5230 Tabs," 2 Aug 2019 (SECRET)[57]
- "Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems"[58]
- Defense Acquisition Guidebook (DAG), Chapter 3, "Systems", 26 May 2017
- Defense Acquisition Guidebook (DAG), Chapter 3-4.3.24, "System Security Engineering", 26 May 2017
- Defense Acquisition Guidebook (DAG), Chapter 7, "Intelligence Support & Acquisition", 26 May 2017
- Defense Acquisition Guidebook (DAG), Chapter 8, "Test and Evaluation", 26 May 2017
- Defense Acquisition Guidebook (DAG), Chapter 9, "Program Protection", 26 May 2017
- Defense Acquisition Guidebook (DAG), Chapter CH 9–3.3 "Engineering Design Activities", 26 May 2017
- Defense Acquisition Guidebook (DAG), Chapter CH 9–4.1 "Contracting for Program Protection", 26 May 2017
- "DoD Anti-Tamper Desk Reference, Second Edition", April 2017 (FOUO)
- "DoD Anti-Tamper (AT) Guidelines", 30 Nov 2016 (SECRET)
- "DoD Anti-Tamper Technical Implementation Guide (TIG)", v1.0 (SECRET), 30 November 2016
- "DoD Cloud Computing Security Requirements Guide", V 1, Release 3, DISA, 6 March 2017
- "DoD Cloud Service Catalog"[59]
- "DoD Critical Program Information (CPI) Horizontal Protection Guidance", v2.0, August 2018
- "DoD Cybersecurity Test and Evaluation (T&E) Guidebook", V 2.0, CH-1, 10 February 2020

[56] **https://at.dod.mil/**
[57] **https://at.dod.mil/**
[58] **https://www.dtic.mil/DTICOnline/home.search**
[59] **https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx** (DoD CAC/PKI required)
http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf (Public)

Guidance (continued)

- DoDM 5200.01 V1, “DoD Information Security Program: Overview, Classification, and Declassification”, 7 July 2020
- DoDM 5200.01 V2, “DoD Information Security Program: Marking Of Information”, 7 July 2020.
- DoDM 5200.01 V3, “DoD Information Security Program: Protection of Classified Information, 8 July 2020
- DoDM 5200.02, CH-1, “Procedures For The DoD Personnel Security Program (PSP)”, 29 October 2020
- DoDM S-5230.28, “Policy for Low Observable (LO) and Counter Low Observable (CLO) Programs", 28 December 2016
- DOT&E Memorandum, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs,” 3 April 2018
- OUSD(A&S) Memorandum, “Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting,” 6 November 2018
- “Cyber Survivability Endorsement Implementation Guide”, v2.0, Appendix X3: Mission-Based Cybersecurity Risk Assessment, JCS, undated, (FOUO)[60]
- “Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)”, 2021
- MIL-HDBK-520, “Systems Requirements Document (SRD) Guidance”, 19 December 2011
- “Mission Engineering (ME) Guide”, OUSD(R&E), November 2020
- “Mission-based Risk Assessment Process for Cyber (MRAP-C) Process Guidebook”, V 2.0, USAF, 1 April 2020
- “Program Protection Plan Outline & Guidance”, v1.0, DASD(SE), July 2011
- “Software Assurance Countermeasures in Program Protection Planning,” DASD(R&E)/DoD CIO, March 2014
- “Trusted Systems and Networks (TSN) Analysis”, DASD (SE)/DoD CIO, June 2014
- “Verification Expectations for Select Section 15 Criteria”, AC-17-01, FAA, 23 March 2017

[60] https://intelshare.intelink.gov/sites/cybersurvivability/

Legal

- 32 CFR 236.4, “Cyber Incident Reporting Procedures”, 1 July 2020
- DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”, 1 December 2019
- DFARS Clause 252.204-7302, “Safeguarding Covered Defense Information and Cyber Incident Reporting Policy”
- FR, Vol. 86, No. 93, Executive Order, “Improving the Nation’s Cybersecurity”, 12 May 2021
- ITAR 22 CFR 120-130, “International Traffic in Arms Regulation (ITAR)[61]
- National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, SEC. 804
- Public Law 111-383 (FY11 NDAA, Section 932): Strategy on Computer Software Assurance
- United States Code (USC) Title 10, § 133a, 133b, 01 February 2018
- United States Code (USC) Title 40, Clinger-Cohen Act

[61] **https://www.pmddtc.state.gov/**

Policy

- AFDP 1, "Air Force Capstone Doctrine”, 10 March 2021
- AFI 10-021, “Force Readiness Reporting”, 22 December 2020.
- AFI 10-601, “Operational Capability Requirements Development”, 6 Nov 2013
- AFI 10-701, “Operations Security” (OPSEC)”, CH-1, 9 June 2020
- AFI 10-701, “Operations Security” (OPSEC)”, AFSC Supplement, 17 March 2008
- AFI 16-1404, “Air Force Information Security Program,” 04 August 2020
- AFI 16-1406, “Air Force Industrial Security Program,” 25 Aug 2015, Incorporating Change 1, 19 December 2017
- AFI 17-101, “Risk Management Framework (RMF) for Air Force (AF) Information Technology,” 06 February 2020
- AFI 17-130, “Cyberspace Program Management,” 13 February 2020
- AFI 17-203, “Cyber Incident Reporting”, 16 March 2017
- AFI 31-101, “Integrated Defense (ID)”, 16 September 2020
- AFI 63-101/20-101, “Integrated Life Cycle Management”, 30 June 2020
- AFI 91-102_AFGM2020-01, “Nuclear Weapon System Safety Studies, Operational Safety Reviews and Safety Rules”, (Immediate Change), 22 May 2019
- AFI 91-202_AFGM2021-01, “The US Air Force Mishap Prevention Program”, 15 April 2021
- AFI 99-103, “Capabilities-Based Test and Evaluation”, 11 December 2020
- AFM 99-113, “Space System Test and Evaluation Process Direction and Methodology for Space System Testing”, 1 May 1996
- AFMAN 14-401, “Intelligence Analysis And Targeting Tradecraft/Data Standards,” 28 October 2019
- AFMAN 16-1405, :Air Force Personnel Security Program”, 1 August 2018
- AFMAN 17-1402, “Air Force Clinger Cohen Act Compliance Guide,” 20 Jun 2018
- AFPAM 63-113, "Program Protection Planning for Lifecycle Management,” 17 October 2013
- AFPAM 63-119, “Mission-Orientated Test Readiness Certification”, 15 April 2021
- AFPAM 63-128, “Integrated Lifecycle Management,” 03 February 2021
- AFPD 33-3, “Information Management”, 21 June 2016
- AFPD 71-1, “Criminal Investigations and Counterintelligence”, 1 July 2019
- AFPD 63-1, “Integrated Lifecycle Management,” 03 Jun 2016, 7 Aug 2018
- AMCI 99-101, “Test and Evaluation Policy and Procedures”, 18 June 2018

Policy (continued)

- CJCSI 5123.01H, “Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS),” 31 August 2018
- CNSSD No. 505, “Supply Chain Risk Management (SCRM),” 29 August 2017
- "Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, p.56157, 4 May 2020
- DoDD 5000.01, “The Defense Acquisition System.” 09 September 2020
- DoDD 5000.71, “Rapid Fulfillment of Combatant Commander Urgent Operational Needs,” 29 May 2020
- DoDD 5105.84, Director (Cost Assessment and Program Evaluation)DoDD 5135.02, “USD (A&S),” 14 August 2020
- DoDD 5205.02E, CH-2, “DoD Operations Security (OPSEC) Program, 20 August 2020
- DoDD 5200.47E, “Anti-Tamper (AT),” 4 September, 2015; Incorporating Change 3, 22 December 2020
- DoD 5220.22-M, “National Industrial Security Program Operating Manual,” 28 Feb 2006, Incorporating Change 2, 18 May 2016
- DoDD 5230.25, “Withholding of Unclassified Technical Data from Public Disclosure” 15 October 2018
- DoDD 5240.02, “Counterintelligence (CI)“, 15 Oct 2013
- DoDD 5250.01, CH-1, 29 August 2017
- DoDD 8570.01-M, "Information Assurance Workforce Improvement Program,” 19 Dec Incorporating Change 4, 10 Nov 2015
- DoDI O-5240.24, “Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)”, CH-2, 15 July 2020
- DoDI S-5230.28, “Low Observable (LO) and Counter Low Observable (CLO) Programs,” 26 May 2005, Incorporating Change 3, 22 December 2020
- DoDI 3200.12, “DoD Scientific and Technical Information Program (STIP)”, CH-3, 17 December 2018
- DoDI 4140.01, “DoD Supply Chain Materiel Management Policy,” 6 Mar 2019
- DoDI 4140.67, “DoD Counterfeit Prevention Policy,” 26 Apr 2013, Incorporating Change 3, 31 Aug 2018 06 March 2020
- DoDI 5000.PR, Human Systems Integration (HSI), 23 January 2020
- DoDI 5000.01, “The Defense Acquisition System,” 09 September 2020
- DoDI 5000.02, Operation of the Adaptive Acquisition Framework. 23 January 2020
- DoDI 5000.73, Cost Analysis Guidance and Procedures, 13 March 2020.
- DoDI 5000.74, “Defense Acquisition of Services,” 10 January 2020
- DoDI 5000.75, Business Systems Requirements and Acquisition, CH-2, 24 January 2020
- DoDI 5000.80, “Operation of Middle Tier of Acquisition (MTA),” 30 December 2019

Policy (continued)

- DoDI 5000.81, Urgent Capability Acquisition, 31 December 2019
- DoDI 5000.82, Acquisition of Information Technology, 21 April 2020
- DoDI 5000.83, Technology and Program Protection to Maintain Technological Advantage, 20 July 2020
- DoDI 5000.84, Analysis of Alternatives, 4 August 2020
- DoDI 5000.85, “Major Capability Acquisition”, USD (A&S), 6 August 2020
- DoDI 5000.86, “Acquisition Intelligence”, USD (A&S)/USD(I&S), 11 September 2020
- DoDI 5000.87, Operation of the Software Acquisition Pathway, 2 October 2020
- DoDI 5000.88, Engineering of Defense Systems, 18 November 2020
- DoDI 5000.89, Test and Evaluation (T&E), 19 November 2020
- DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers, 31 December 2020
- DoDI 5010.44, “Intellectual Property (IP) Acquisition and Licensing”, 16 October 2019
- DoDI 5200.39, “Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)”, CH-3, 01 October 2020
- DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”, CH-2, 15 October 2018
- DoDI 5200.47, CH-3, “Anti-Tamper (AT)”, 22 December 2020
- DoDI 5200.48, “Controlled Unclassified Information (CUI)”, 6 March 2020
- DoDI 5220.22, “National Industrial Security Program (NISP)”, CH-2, USD(I&S), 24 September 2020
- DoDI 5230.24, “Distribution Statements on Technical Data”, CH-3, 15 October 2018
- DoDI 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” CH-2, 11 December 2019
- DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT), CH-3, DoD (CIO), 29 December 2020
- GAO-20-48G TRA Guide, “Technology Readiness Assessment Guide”
- MDA 5200.08-M, Encl. 3
- "National Space Traffic Management Policy", Federal Register, Vol. 83, No. 120, Space Policy Directive 3, p. 28969, 21 June 2018
- NSTISSAM TEMPEST/1-92, “Compromising Emanations Laboratory Test, Electromagnetics,” 15 Dec 1992
- OUSD Memorandum, “Software Acquisition Pathway Interim Policy and Procedures”, 03 Jan 2020

Reports

- “GAO-21-179, “Weapon Systems Cybersecurity - Guidance Would Help DOD Programs Better Communicate Requirements to Contractors”, p. 26, March 2021

Standards

- CNSSI 1253, “Security Categorization and Control Selection for National Security Systems”, 27 Mar 2014
- CNSSI No. 4009, “Committee on National Security Systems (CNSS) Glossary,“ 6 April 2015
- FIPS 140-2, “Security Requirements for Cryptographic Modules,” 22 March 2019
- FIPS 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” Aug 2013IEEE 15288.2, “Standards for Technical Reviews and Audits on Defense Programs”, 15 May 2015
- ISO/IEC/IEEE Standard 15288, “Systems and Software Engineering,” 05 May 2015
- ISO 17666:2016, “Space Systems – Risk Management”, 1st Ed., 01 November 2016
- MIL-STD-882E, “Department of Defense Standard Practice: System Safety”, 11 May 2012
- NIST SP500-292, "NIST Cloud Computing Reference Architecture", September 2011
- NIST SP500-293, "US Government Cloud Computing Technology Roadmap Volume I, High-Priority Requirements to Further USG Agency Cloud Computing Adoption', October 2014
- NIST SP800-30, “Guide for Conducting Risk Assessments,” Rev 1, Sep 2012
- NIST SP800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems,” Dec 2018
- NIST SP800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 5, 23 10 December 2020
- NIST SP800-59, “Guideline for Identifying an Information System as a National Security System,” 20 August 2003
- NIST SP800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” Sep 2011
- NIST SP800-145, "The NIST Definition of Cloud Computing", September 2011
- NIST SP800-160, Volume 1, “Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems,” Nov 2016
- NIST SP800-160, Volume 2, “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”, Nov 2019
- NIST SP800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” Apr 2015
- NIST SP800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” Rev. 2, 7 June 2018 28 January 2021
- NIST SP1500-201, “Framework for Cyber-Physical Systems: Volume 1, Overview”, v1.0, June 2017.
- NIST SP1500-202, “Framework for Cyber-Physical Systems: Volume 2, Working Group Reports”, v1.0, June 2017.
- NISTIR 8053, “De-Identification of Personal Information”, 16 January 2020
- SMC-S-014 (2010), “AFSC Standard: Survivability Program Management for Space”, 19 July 2010

Tools

- Centralized Cyber Capabilities Directory (C3D)[62]
- Department of Defense Procurement Toolbox
- PM Toolkit[63]
- USAF Evaluated Product List (EPL)

[62] **https://rdte.services.nres.navy.mil/C3D/**
[63] **https://hanscomnet.hanscom.af.mil/pmtb/MR/MR.html**

Training

- AFLCMC hosts a 3-Day Program Protection Training class, available quarterly, with a Distance Learning option available during the course.[64]
- DAU Training Catalog[65]
- Defense Acquisition University offers a 12-hour ACQ 160 Program Protection Planning Awareness course[66]

[64] **https://www.milsuite.mil/book/groups/acquisition-program-protection-planning**
[65] **https://icatalog.dau.edu/onlinecatalog/CareerLvl.aspx**
[66] **https://icatalog.dau.edu/onlinecatalog/courses.aspx?crs_id=2082**

USAF SSE CYBER ENGINEERING GUIDEBOOK REFERENCE RESOURCES
ACADEMIC PAPERS
https://ieeexplore.ieee.org/Xplore/home.jsp
https://www.jstor.org/
https://www.omicsonline.org/peer-reviewed-journals.php
https://www.researchgate.net
DoD CODES, LAWS & REGULATIONS
https://www.acq.osd.mil/dpap/pdi/cyber/index.html
DoD FORMS & TOOLS
https://dodprocurementtoolbox.com/
https://www.esd.whs.mil/DD/admin_inst/
DoD GUIDEBOOKS & HANDBOOKS
https://www.dote.osd.mil/Publications/DOT-E-TEMP-Guidebook/
DoD INSTRUCTIONS & DIRECTIVES
https://www.defense.gov/Resources/Forms-Directives-Instructions/
https://www.esd.whs.mil/Directives/issuances/DoDI/
STANDARDS AND SPECIFICATIONS
http://everyspec.com
https://quicksearch.dla.mil/qsSearch.aspx
https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/
UNITED STATES GOVERNMENT CODES, LAWS & REGULATIONS
https://search.usa.gov/search?utf8=%E2%9C%93&affiliate=www.acq.osd.mil&query=DFARS+204.7501

USAF SSE CYBER ENGINEERING GUIDEBOOK REFERENCE RESOURCES
https://uscode.house.gov/browse.xhtml;jsessionid=56AA6B4AE83BA3D3E86E8AD739D48E58
https://www.acquisition.gov/
https://www.ecfr.gov/cgi-bin/searchECFR?idno=32&q1=2002&rgn1=PARTNBR&op2=and&q2=&rgn2=Part
https://www.govinfo.gov/
UNITED STATES GOVERNMENT INSTRUCTIONS & DIRECTIVES
https://www.cnss.gov/CNSS/issuances/Policies.cfm
UNITED STATES GOVERNMENT REPORTS & STUDIES
https://www.govinfo.gov/app/search/%7B%22query%22%3A%22reports%20studies%22%2C%22offset%22%3A0%7D
USAF GUIDEBOOKS & HANDBOOKS
https://acqnotes.com/dod-guides-handbooks
https://www.afacpo.com/apm/
https://www.e-publishing.af.mil/
USAF DIRECTIVES, INSTRUCTIONS & MEMORANDUMS
https://www.afacpo.com/apm/
https://www.e-publishing.af.mil/

APPENDIX J

TEMPLATES

Attack Path Analysis Template

Attack Path
Vignette Template (N

Refer to Appendix D for the proper use of the Attack Path Vignette Template.

NOTE: Future additions to this Appendix will be a workbook for the DoD Survivability KPP, KSA, and APA through their CIA levels as assigned to the latest NIST RMF Control families and individual controls as the means of recording the architectural baseline cybersecurity controls within a space and weapon system family's TMS. Pending changes to the existing three Cyber Principles (Cybersecurity, Cyber Resiliency and Cyber Survivability) from the DoD are forthcoming, hence the delay in providing this useful Excel-based tool for the reader.

USAF SSE Cyber Guidebook Comments Resolution Matrix (CRM)

USAF SSE Cyber
Guidebook CRM Ter

Comments, suggestions, or questions on this document should be captured in CRM.

Email CRMs to the Cyber Resiliency Office for Weapon Systems, Acquisition Support Team, System Security Engineering Lead, Ms. Katie Whatmore NH-04 USAF AFMC AFLCMC/EN-EZ/CROWS

(**katie.whatmore@us.af.mil**).

Quia Omnis Mollitia
CROWS
Cyber Resiliency Office For Weapon Systems