United States Air Force

Weapon System
Program Protection / Systems Security Engineering
Guidebook

Version 2.0

12 March 2020

Approved:

BRADLEY.JOSEPH.F.JR.1253989625 Digitally signed by BRADLEY.JOSEPH.F.JR.1253989625 Date: 2020.03.12 10:44:19 -04'00'

JOSEPH F. BRADLEY, JR., SES, DAF
Director, Cyber Resiliency Office for Weapon Systems

ENDORSEMENTS

This guidebook has been coordinated with and endorsed by the following organizations:

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

FOREWORD

1. To effectively execute the activities of this guidebook, 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 experience level. DAU certification standards and required acquisition courses are listed here:

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

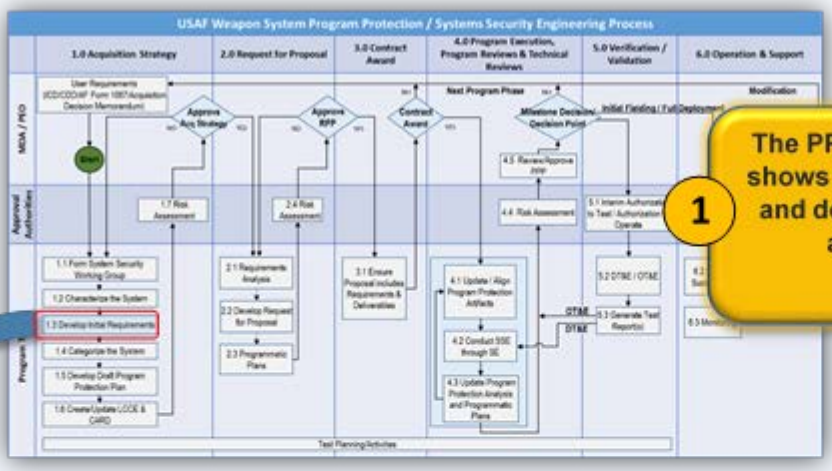
2. Comments, suggestions, or questions on this document should be submitted on a Comments Resolution Matrix (CRM) form and emailed to the Cyber Resiliency Office for Weapon Systems (CROWS@us.af.mil). The Comments Resolution Matrix form is in Appendix K.

RECORD OF CHANGES

Version	Effective Date	Summary
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

This Guidebook is intended to assist program offices in performing the engineering analysis needed to understand the cyber-related aspects of their weapon systems. It encompasses a holistic look at different aspects of cyber (Cybersecurity, Trusted Systems and Networks, Anti-Tamper, Information Protection, Cyber Resiliency), and outlines a single process to better integrate Program Protection (PP) and Systems Security Engineering (SSE) activities into traditional Systems Engineering processes – with the goal of helping program offices design their weapon systems to be more cyber resilient.



1 The PP/SSE Process Flowchart shows the order of all processes and decision points across the acquisition lifecycle (Page 7)

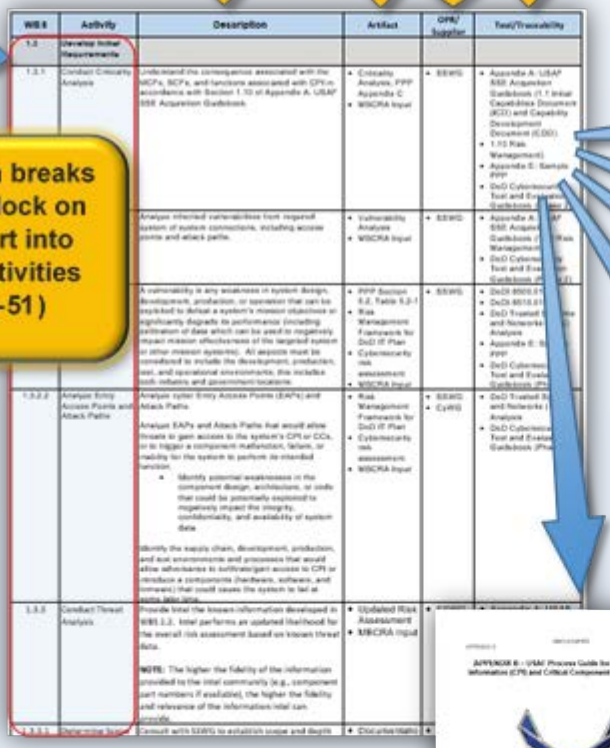
2 The WBS then breaks down each block on the Flowchart into individual activities (Pages 13-51)

ACTIVITY DESCRIPTION

ARTIFACTS PRODUCED

OPR

REFERENCES



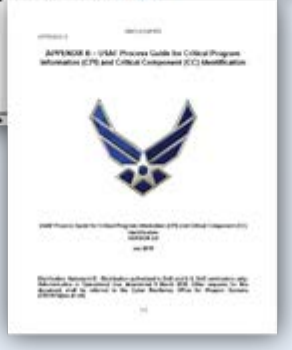
3 Many references are attached as appendices – these give more detail on how to accomplish each activity

CPI/CC Identification Guide

Functional Thread Analysis

Aircraft Use Case

Sample Program Protection Plan (PPP)



USAF SSE Acquisition Guidebook

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

TABLE OF CONTENTS

APPENDIX SUMMARY:

APPENDIX A - USAF SSE Acquisition Guidebook

Formerly a separate document, this Guidebook has been updated and is included here as it is referenced for additional guidance throughout the main document. Future releases of the USAF SSE Acquisition Guidebook will no longer be a separate publication, but will continue to be updated and released as part of this combined guidebook.

APPENDIX B – USAF Process Guide for CPI and CC Identification

Formerly a separate document, this Process Guide has been updated and is included here as it is referenced for additional guidance on various topics in the main document. Future releases of the USAF Process Guide for CPI and CC Identification will no longer be a separate publication, but will continue to be updated and released as part of this combined guidebook.

APPENDIX C – Functional Thread Analysis & Attack Path Analysis

Additional information on how to perform a system functional decomposition to identify mission and safety critical functions and identify potential cyber-attack paths.

APPENDIX D – Example Use Cases

A worked example of a fictitious aircraft system development to help the reader understand how to apply the PP/SSE Process within this document. Further use cases planned for other types of weapon systems.

APPENDIX E – Sample Program Protection Plan (PPP)

A generic vehicle example to show how the artifacts outputted from the PP/SSE Process in this document are used to meet PPP requirements.

APPENDIX F – 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 G – Relationship to Other Processes

Mapping of the PP/SSE Process to the Risk Management Framework (RMF) and the Mission Based Cyber Risk Assessment (MBCRA) process.

APPENDIX H – Definitions

APPENDIX I – Acronym List

APPENDIX J – References

APPENDIX K – Comments Resolution Matrix

Executive Summary

This guidebook provides single source guidance on Systems Security Engineering (SSE) within the United States Air Force (USAF) weapons system acquisition community.

The process described in this document distills all the requirements from applicable policies to support consistent contract language and process through the acquisition life cycle. Additionally, this process accounts 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 G.

In this guidebook, weapons systems are 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, but exclude supporting infrastructure and Information Technology (IT) systems.

This guidebook was developed to:

- Provide a common starting point for acquisition category (ACAT) and National Defense Authorization Act (NDAA) Section 804 programs to ensure SSE is an integral aspect of program management and systems engineering and that the required acquisition documents and artifacts are developed to support the required approval timelines. This will facilitate the development of well-defined and complete plans and schedules for use in program execution, thereby reducing risks and increasing the probability of program success.
- Provide a consistent approach and process for developing weapon systems that applies systems engineering principles in a standardized, repeatable, and efficient manner to identify security vulnerabilities, requirements, and verifications that minimize risks. This guidebook includes guidance on SSE process applications and provides detailed, comprehensive cybersecurity and cyber resiliency requirements for weapon systems.
- Improve USAF-critical, enterprise-wide weapon system risk 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 acquisition process.
- Promote the development by vendors of trustworthy, secure software 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 the life cycle.
- Allow tailoring to each program’s or project’s specific needs

The guidance in this document should be tailored and scaled according to the size and content of the program. Reference documents for this guidebook are included in the appendices.

1.0 Background.

1.1 The Task Force Cyber Secure Establishment memorandum, dated 20 Mar 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.

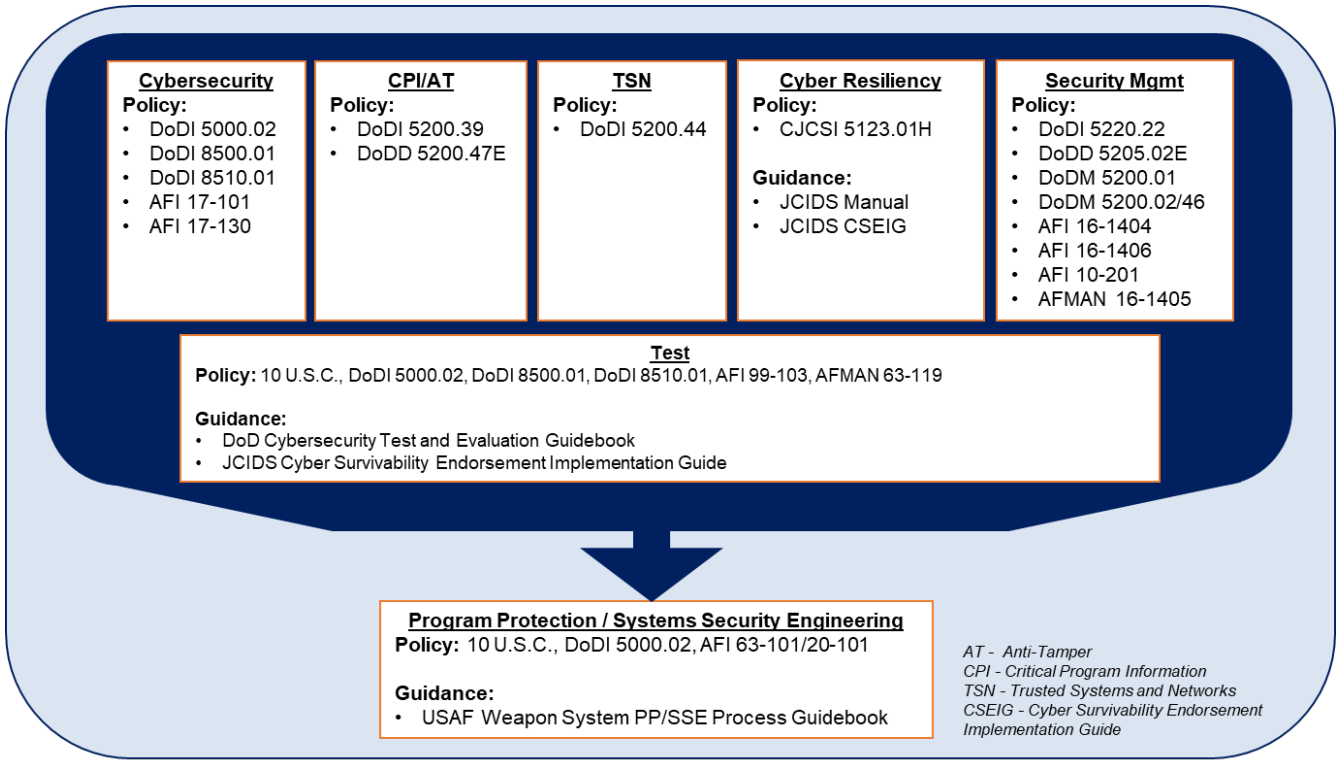


FIGURE 1: Program Protection and Systems Security Engineering Policy.

1.2 Relevant policy excerpts:

1.2.1 Bottom Line Up Front: The process described in this document has distilled all the requirements from the relevant security policies to help provide consistent security-related contract language and a consistent process for integrating all security-related requirements into the Systems Engineering process to ensure they are traded appropriately against all other system requirements. The policy excerpts below show this is not a new requirement for weapon system programs.

1.2.1.1 10 U.S.C., § 2224

- *The DoD must ensure the "availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure." This includes "vulnerability and threat assessment[s] of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the Armed Forces."*

1.2.1.2 Department of Defense Instruction (DoDI) 5000.02, Enclosure 11, *Requirements Applicable to All Programs Containing Information Technology (IT)*

- *6. CYBERSECURITY.*

  Cybersecurity Risk Management Framework (RMF). Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01 (Reference (bg)), should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, system engineering, and test and evaluation. Integration of the RMF in acquisition processes reduces required effort to achieve authorization to operate and subsequent management of security controls throughout the system life cycle.

1.2.1.3 DoDI 5000.02, Enclosure 14, *Cybersecurity in the Defense Acquisition System*

- *Para b. Design for Cyber Threat Environments. In order to design, develop, and acquire systems that can operate in applicable cyber threat environments, Program Managers will:*

- *(1) Derive cybersecurity and other system requirements into system performance specifications and product support needs*

1.2.1.4 DoDI 8510.01, Enclosure 6, *Step 3 - Implement Security Controls.*

- *Para 2, c, 1, (c) The ISO or PM/SM must ensure early and ongoing involvement by IS security engineers qualified in accordance with DoD 8570.01-M (Reference (z)). Mission owner(s) must translate security controls into system specifications into the system design, and ensure security engineering trades do not impact the ability of the system to meet the fundamental mission requirements. This includes ensuring that technical and performance requirements derived from the assigned security controls are included in request for proposals and subsequent contract documents for design, development, production, and maintenance.*

1.2.1.5 AFI 63-101/20-101, *Integrated Life Cycle Management.*

- *6.2.1 Security-related system requirements are fully derived and integrated into overall system requirements, incorporated into the system's design through systems' security engineering (SSE), and thoroughly tested from a mission perspective.*

- *6.2.2 Security-related program requirements are included in RFP and contract language, to include requirements and evidence of a secure supply chain (e.g., statistical part inspections, facility inspection results, network certifications).*

1.2.1.6 AFI 99-103, *Capabilities*-based *Test and Evaluation*

- *The fundamental purpose of T&E is to ensure DoD acquires systems that work and meet specified requirements. Additionally, overarching functions of T&E are to mature system designs, manage risks, identify and help resolve deficiencies as early as possible, assist in reducing unintended cost increases during development,*

operations, and throughout the system life cycle, and ensure systems are operationally mission capable (i.e., effective, suitable, survivable, and safe).

- *Cyber test planning must be integrated across the entire program lifecycle, [including] the requirements generation process and the system engineering process, yielding requirements that are testable and achievable, and test plans that provide actionable capabilities-oriented test results.*
- *Cyber test includes both cybersecurity testing (system defense against cyber-attack) and cyber resiliency testing (system detection and response if defense is defeated).*

1.2.2 Programs are encouraged to design weapon systems for cyber survivability through the direction of DoDI 5000.02 and the Joint Capabilities Integration and Development System (JCIDS). These documents require Cyber Survivability to be included as a part of the mandatory key performance parameter (KPP) of System Survivability (SS). Cyber Survivability, one of three focus elements under the SS KPP, is the ability of a system to prevent, mitigate and recover from cyber-attacks. This guidebook will aid program offices with how to integrate Cyber Survivability into their weapon system requirements.

1.2.2.1 DoDI 5000.02, Enclosure 14, paragraph 3 (b) also elaborates that Program Managers will ensure systems are designed to operate in cyber threat environments, and they will do so by using the capability development document (CDD) to inform requirements derivation activities and "*ensure KPPs and attributes establish system survivability*". Since Cyber Survivability is one of the three focus elements of the mandatory System Survivability (SS) KPP in the CDD (as described in The Manual for the Operation of the JCIDS, in paragraph 2.2 of Annex C to Appendix G to Enclosure B), this guidebook can aid Program Managers in ensuring systems are designed for cyber survivability.

2.0 Scope.

2.1 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 needs for weapon system operation in today's cyber-contested environments. One method of doing this is by using SSE processes to design systems in a way that makes them more resilient to cyber-attacks.

2.2 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 weapon systems to operate in cyber-contested environments in order to complete their missions.

NOTE: 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 USAF Weapon System Program Protection (PP) / Systems Security Engineering Guidebook is the starting point for the acquisition professional to understand the activities/tasks and timelines to execute PP and SSE throughout the SE process.

2.3 The USAF Weapon System PP/SSE Guidebook enables both Acquisition Category (ACAT) programs and NDAA 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).

2.4 The USAF Weapon System PP/SSE Guidebook serves as the integrating process for implementing, as appropriate, the following security countermeasures to weapon systems IAW DoD Instruction (DoDI) 5000.02, Enclosure 3 and DoDI 5200.44:

- 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)

2.5 The USAF Weapon System PP/SSE Guidebook 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 weapon systems.

2.6 This guidebook, along with Appendix A: USAF SSE AG, 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 weapon system for “new start” programs as well as modification/modernization programs. Application of the process should be based on the milestone/phase the program is executing.

2.7 Appendix D of this guidebook contains two separate use cases for a fictitious aircraft system (new start program and modification program). These use cases demonstrate the processes and activities described in this guidebook using a specific weapon system example.

3.0 Program Protection Plan (PPP) Coordination and Approval.

3.1 By executing the process in this guidebook, artifacts will be generated that will populate the Program Protection Plan. A sample PPP is available in Appendix E and DoD guidance on minimal content is identified in the 'Program Protection Plan Outline – July 2011' available at http://acqnotes.com/acqnote/careerfields/program-protection-plan. The PPP is a living document, approved at program milestones, by the cognizant Milestone Decision Authority (MDA).

3.2 At the beginning of the approval process, the program coordinates the initial/draft PPP with the following governance authorities: Authorizing Official (AO), Trusted Systems and Networks (TSN) Focal Points, Anti-Tamper Executive Agent (ATEA), and Security Management/Information Protection (IP). For final approval, the PPP is coordinated in accordance with Table 1 below, based on the appropriate MDA.

TABLE 1: PPP Coordination and Approval

Milestone Decision Authority	Coordination
Defense Acquisition Executive (DAE)	1. Route the initial/draft of the PPP for review/coordination with stakeholders internal and external (e.g., AO, TSN, ATEA, and IP) to the PEO. 2. 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. 3. 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). 4. Route the SAE-signed PPP to OSD for Final PPP review and approval.
Service Acquisition Executive (SAE)	1. Route the initial/draft of the PPP for review/coordination with stakeholders internal and external (e.g., AO, TSN, ATEA, and IP) to the PEO. 2. 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)	1. Route the initial/draft of the PPP for review/coordination with stakeholders internal and external (e.g., AO, TSN, ATEA, and IP) to the PEO. 2. PEO reviews and approves the PPP.

4.0 PP/SSE Process.

4.1 USAF Weapon System PP/SSE Process.

4.1.1 Figure 3 depicts the Weapon System PP/SSE Process. There are three different lanes (horizontal rows) in the process (MDA/PEO, Approval Authorities, and Program Team). The lanes represent responsibility for the activities. The process is iterative and outlines specific activities to be completed for the following sections (vertical columns):

1.0 Acquisition Strategy.

2.0 Request for Proposal (RFP).

3.0 Contract Award.

4.0 Program execution, Program Reviews & Technical Reviews.

5.0 Verification/Validation.

6.0 Operations and Support.

4.1.2 The blocks within the flowchart are numbered to correspond with these sections above (e.g. 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 flowchart is further decomposed into process activities (e.g. 2.1 “Requirements Analysis” includes process activity 2.1.1 “Finalize Contractor Requirements”).

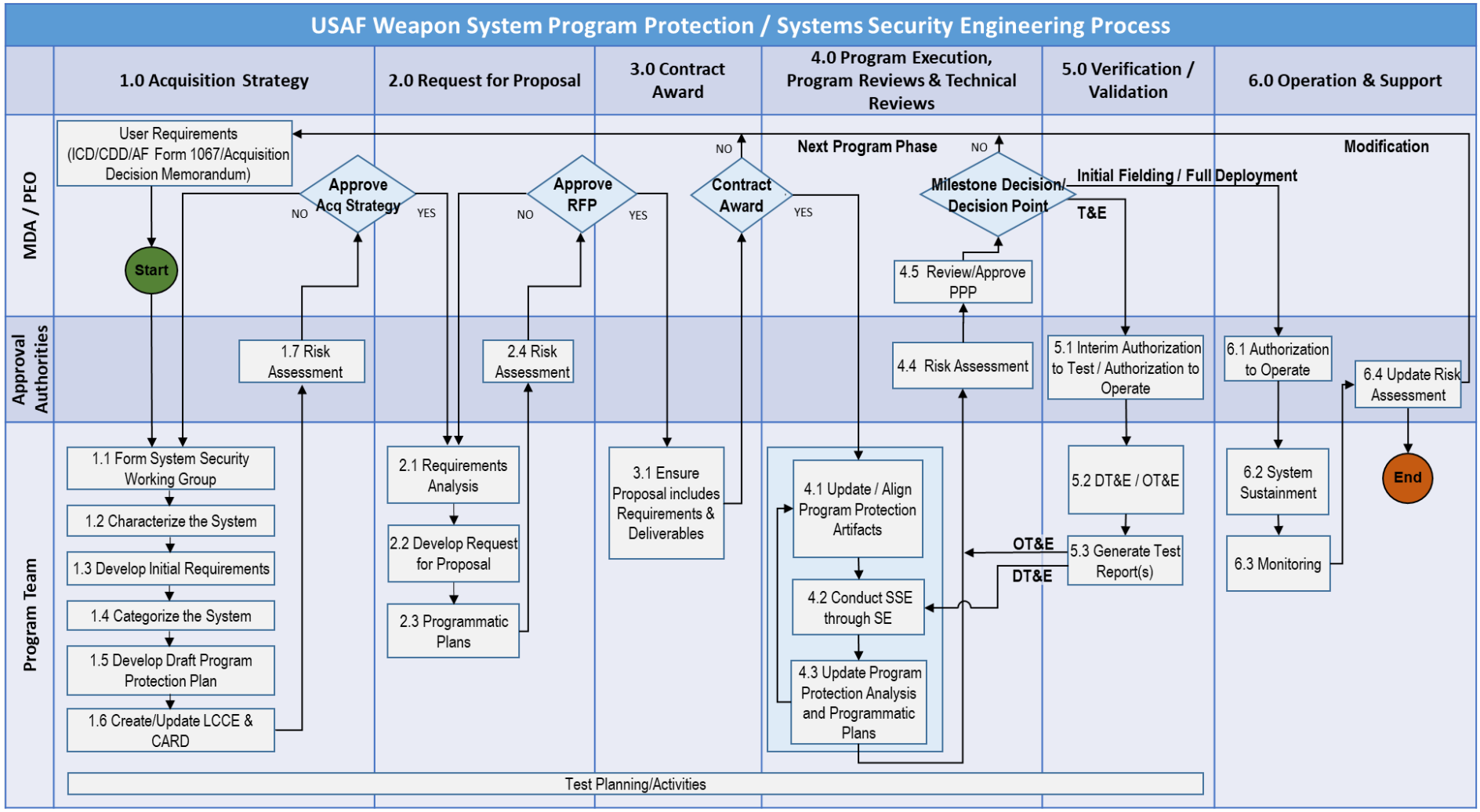


FIGURE 3: USAF Weapon System PP/SSE Process.

4.2 PP/SSE Process and the Acquisition Life Cycle.

4.2.1 Weapon System PP and SSE should be applied continually throughout the acquisition life cycle (see Figure 4 through Figure 10) as many times as necessary. Figure 5 highlights that the process is initiated through receiving a user requirements document. The user requirements may be in the form of an Initial Capabilities Document (ICD), Capabilities Design Document (CDD), AF Form 1067, or Acquisition Decision Memorandum. Requirements from the ICD and CDD will be developed per the JCIDS process, and therefore will drive the need to satisfy the ten Cyber Survivability Attributes (CSAs). 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. More information on the user requirements and the CSAs can be found in Appendix A: USAF SSE Acquisition Guidebook.

4.2.2 The PP/SSE process can be used for a new weapon system development or a modification to an existing weapon system. The need to reapply the PP/SSE process within this guidebook 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. Notice the "Milestone Decision/Decision Point" after step 4.5 in Figure 3 (see also Figure 8) leads to verification/validation, 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 MS B, allowing the program to proceed to the Engineering and Manufacturing Development Phase (EMD). At this point, the program should reevaluate the acquisition strategy, ensure appropriate expertise is included in the Systems Security Working Group (SSWG), and continue progressing through the process again. Typically, the program will then have an EMD contract award and the program will have to leverage lessons learned from the previous milestone and place the proper requirements on contract.

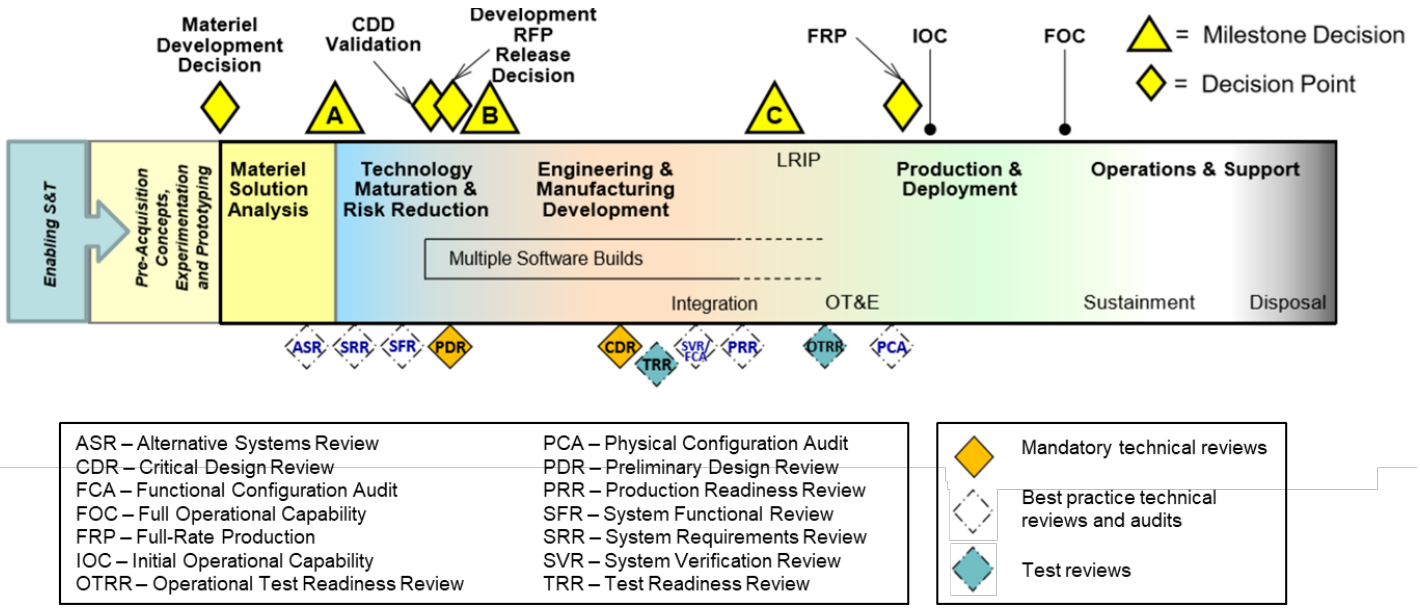


FIGURE 4: Acquisition Life Cycle.

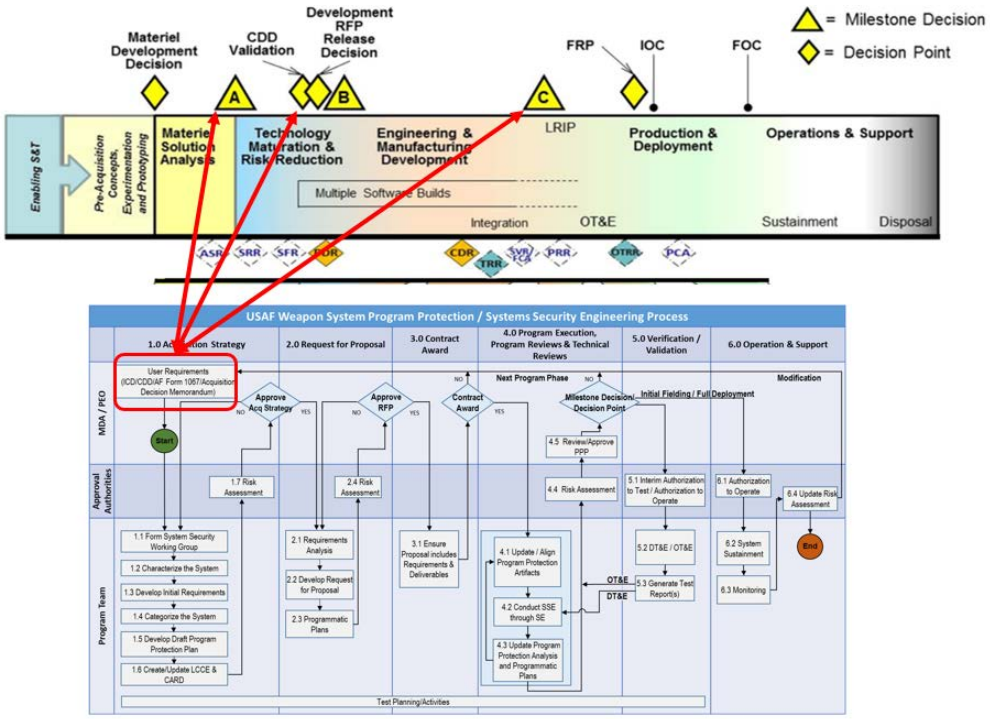


FIGURE 5: User Requirements Aligned to Acquisition Life Cycle.

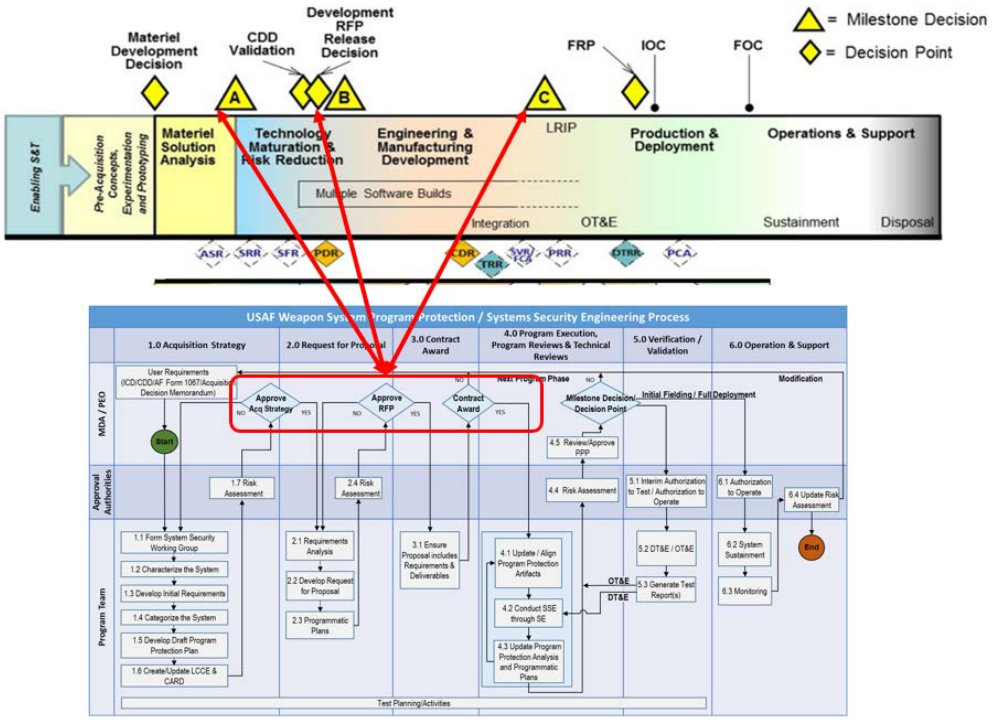


FIGURE 6: Acquisition Strategy, RFP, and Contract Award Aligned to Acquisition Life Cycle.

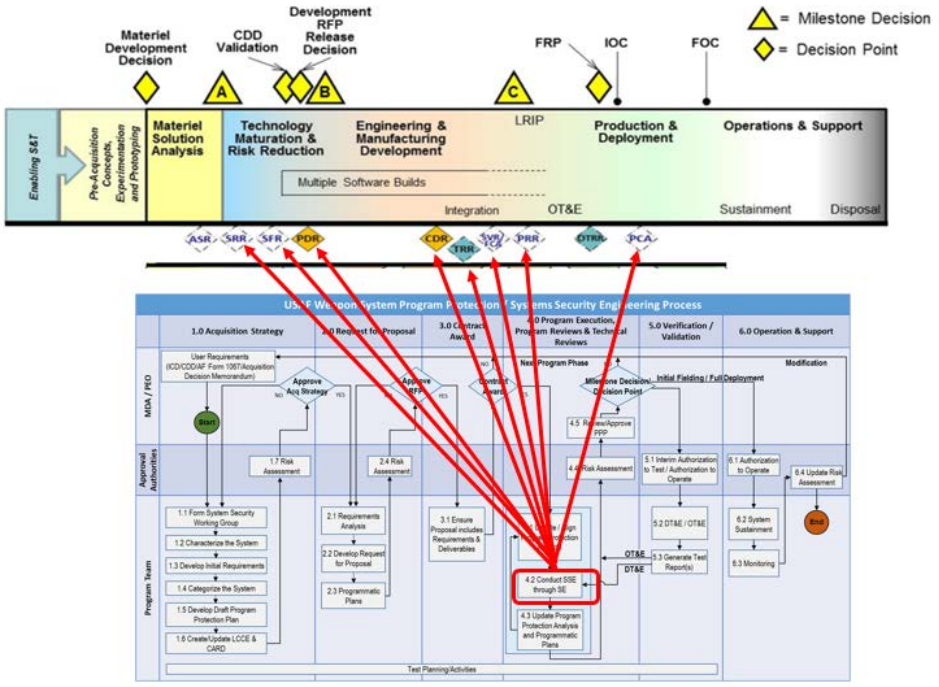


FIGURE 7: Conducting SSE through SE Aligned to Acquisition Life Cycle.

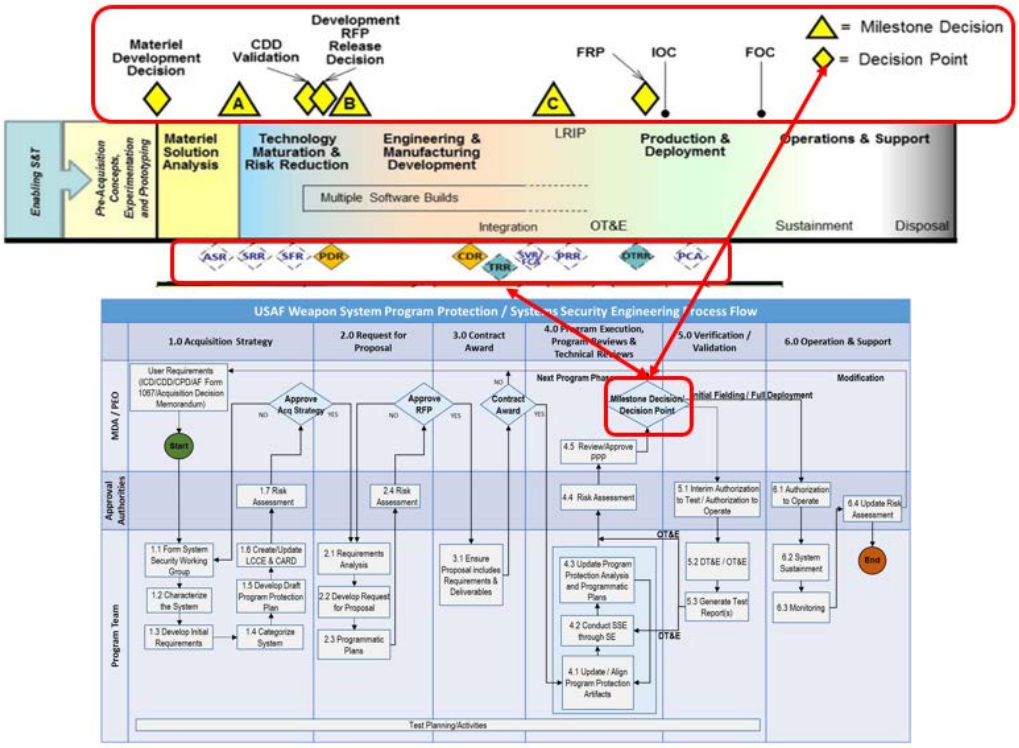


FIGURE 8: Milestone Decisions/Decision Points Aligned to Acquisition Life Cycle.

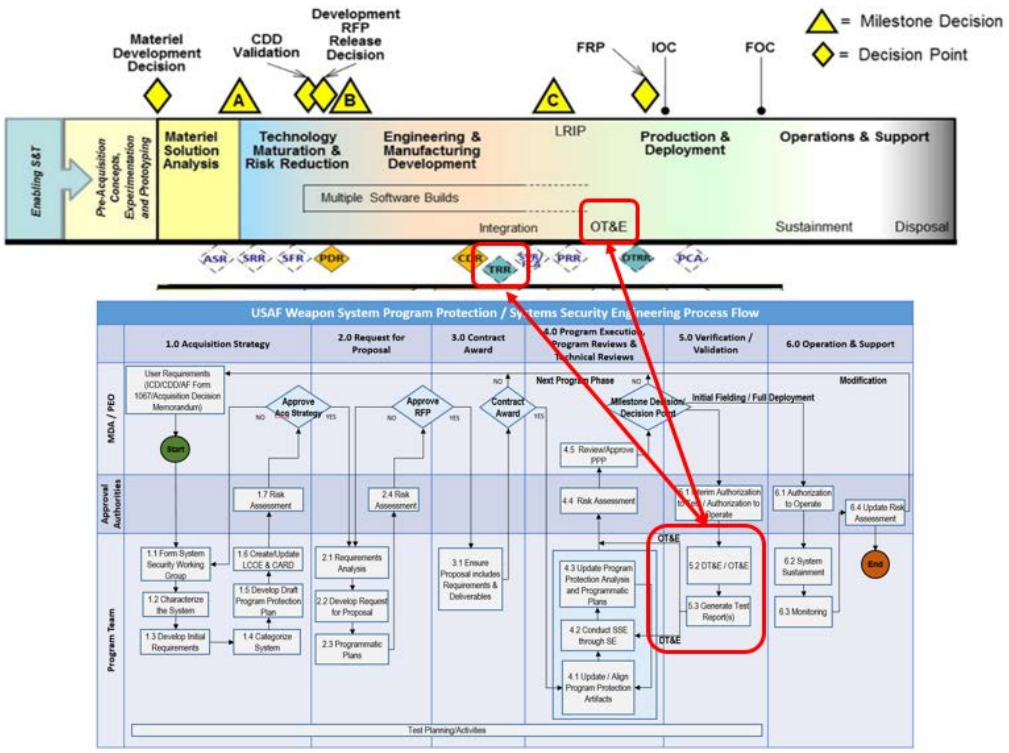


FIGURE 9: Test and Evaluation Aligned to Acquisition Life Cycle.

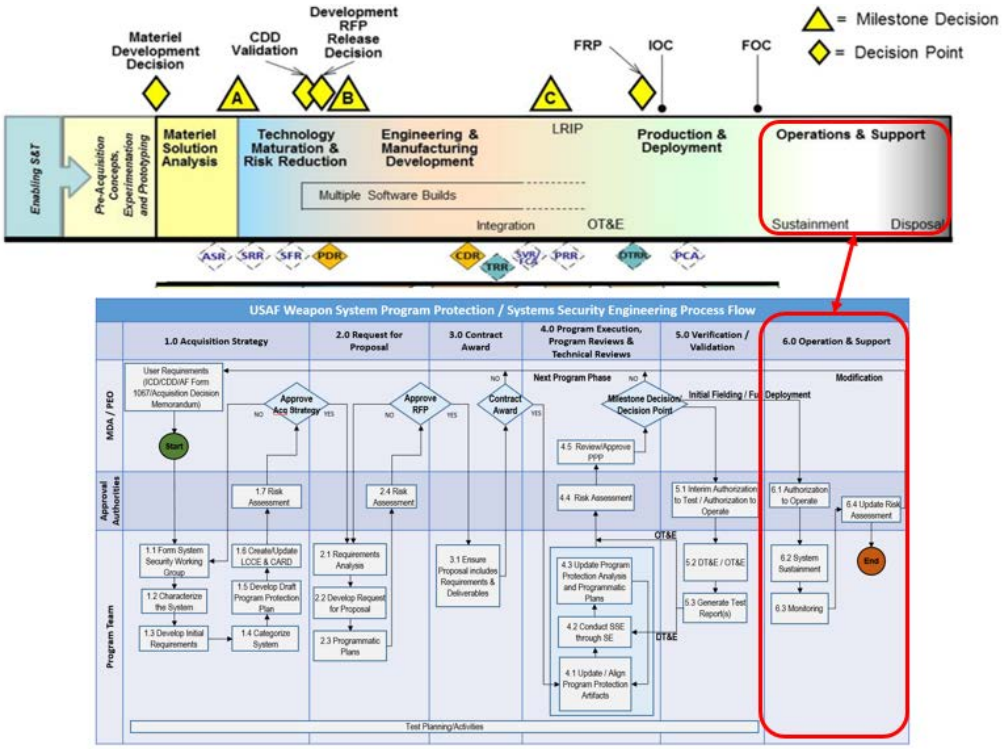


FIGURE 10: Operations & Support Aligned to Acquisition Life Cycle.

4.3 PP/SSE Process and the Systems Engineering "V".

4.3.1 The systems engineering "V" in Figure 11 is the engineering approach for progressing through the acquisition life cycle. Section 4.0 in the WBS decomposes PP and SSE systems engineering activities to be accomplished during the acquisition life cycle. Completing SSE through the SE process is critical to ensuring cybersecurity and resiliency is obtained and maintained through the life cycle of a program.

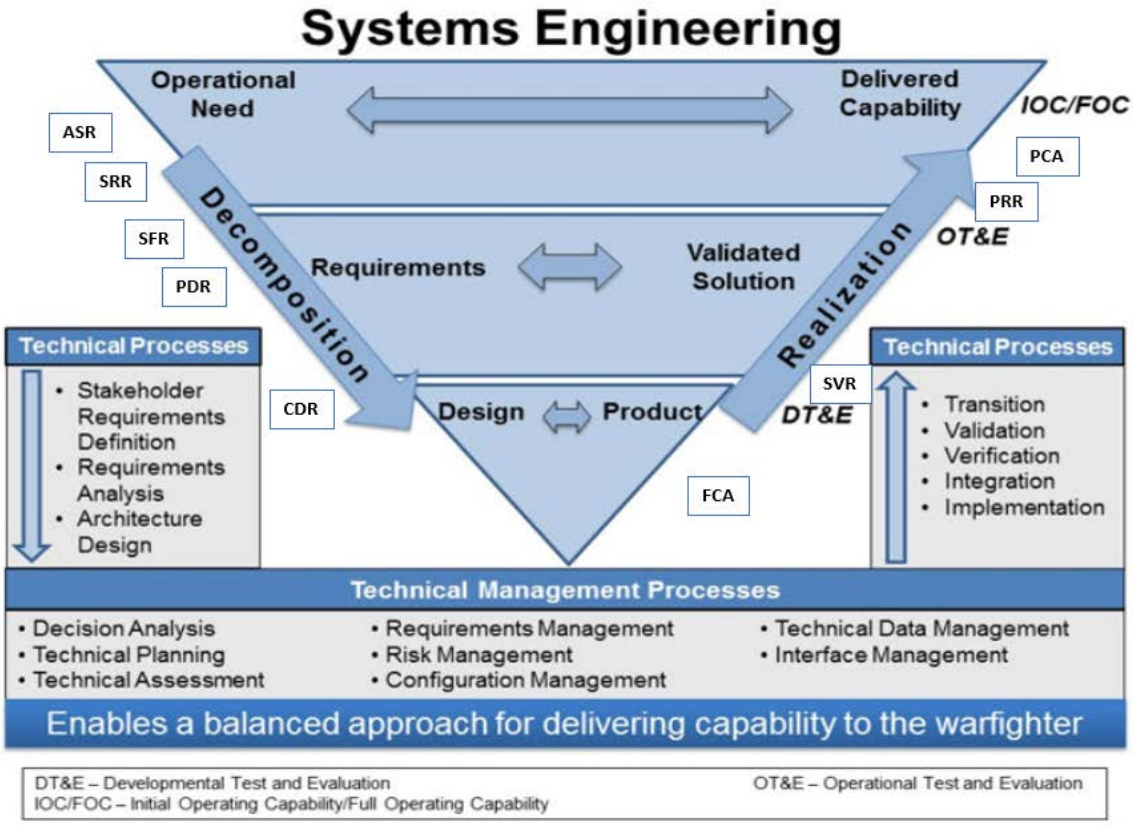


FIGURE 11: Systems Engineering "V".

4.4 Work Breakdown Structure.

4.4.1 The Work Breakdown Structure (WBS) in Table 2 provides additional detail for each of the high-level activities within the process shown on Figure 3.

4.4.1.1 **Activity** – Individual tasks to be accomplished.

4.4.1.2 **Description** – Details on how to execute each activity.

4.4.1.3 **Artifacts** – Documents created/updated during the execution of each activity.

4.4.1.4 **OPR/Supplier** – Organization, team, or individual who has primary responsibility to execute or supply information for each activity.

4.4.1.5 **Tool/Traceability** – References for tools, documents, procedures, or other guidance to aid in completing each activity.

TABLE 2: Work Breakdown Structure (WBS) for the USAF Weapon System PP/SSE Process.

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
	User Requirements	Form High Performance Team (HPT). Provide tailored Cyber Survivability Attribute (CSA) requirements per each critical weapon system function in accordance with the Cyber Survivability Endorsement Implementation Guide.	• ICD/CDD/AF Form 1067/Acquisition Decision Memorandum	• User (MAJCOM) • Program Office • SSE	• Appendix A: USAF SSE Acquisition Guidebook (1.1 ICD, CDD) • Cyber Survivability Endorsement Implementation Guide
1.0	**Acquisition Strategy**				
START	**Enter DoD Acquisition Life Cycle**	Upon entering the DoD Acquisition Life Cycle for any 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 participants should include at least 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), and representatives from the Cybersecurity Working Group (CyWG), AO, TSN, ATEA, and IP.	• PPP Table 1.2-1	• PM	• DoDI 8510.01 • DoDI 5000.02 • DoDI 8500.01 • AFI 99-103 • AFMAN 63-119 • AFPAM 63-113 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP • OSD PPP Outline & Guidance • DoD Cybersecurity Test and Evaluation Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		NOTE: The CyWG should be established 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.			
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, A2.1.3 • Appendix E: Sample PPP
1.1.3	Gather Documentation	Collect relevant/available documentation to assist with the subsequent steps in the process. Review and understand the customer requirements, capabilities, and desired effects. If modifying an existing system, review previously identified vulnerabilities of the system. (Initial Capabilities Document (ICD), Capability Development Document (CDD), CONOPS, System Requirements Document (SRD), Systems Engineering Plan (SEP), top-level	• PPP Section 1.1	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		architecture, previous cyber test results/reports, etc.)			
1.1.4	Intelligence and Counter-intelligence Documentation	Request the appropriate threat information/products respective to the maturity of the program (e.g. 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	• Defense Acquisition Guide (DAG) Chapter 7 • DoDI 5000.02 • DoDD 5240.24 • DoDI 5240.04 • AFPAM 63-113 • Standard Process for Intel Mission Data • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1)
1.1.5	Conduct Information Analysis	Conduct the appropriate activities in order to identify, understand, and protect information about the program and information residing in the system being acquired. 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-V4 • DoD 5220.22-M • Appendix E: Sample PPP • 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. (ICD (CSAs), CDD (CSAs), CONOPS/CONEMP, SRD, etc.). During the JCIDS document approval cycle, ensure that SSWG representation is part of the High Performance Team (HPT). 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 appropriately.	• Acquisition Strategy • CDD • MBCRA Input	• User • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 ICD, CDD) • Appendix B: USAF Combined Process Guide for CPI and CC Identification • 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)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		NOTE: The requirements need to be testable and measurable. This review is also the first step to beginning the Mission Based Cyber Risk Assessment (MBCRA) for test and evaluation.			
1.2.2	Develop System Description	Provide a high-level description of the system and the technology of which it's comprised. Describe the system (including system boundaries and interconnections). For external interconnections, determine requirements needed to achieve Authorization to Operate (ATO)	• PPP Section 1.0 and Appendix E, Cybersecurity Strategy (CS) • MBCRA Input	• SSWG	• DoDI 8510.01 • AFPAM 63-113 • National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP • 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. Include system-unique maintenance/test equipment and training systems if applicable.	• PPP Section 1.1 • MBCRA Input	• SSWG	• 10 U.S.C., DoDI 5000.02, AFI 99-103 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
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. **NOTE:** Based on maturity of program, details of the internal and external boundaries may or may not be known. If	• PPP Section 1.1 and Appendix E • MBCRA Input	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		unknown, ensure bounding the system is started no later than SFR. System boundaries should be updated as more information becomes available.			
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 (i.e., 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. **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 also continue throughout the life cycle of the program.	• PPP Section 2.2, Table 2.2-1, Section 3.0 and Section 4.0 • Anti-Tamper Plan • MBCRA Input	• SSWG	• DoDI 5200.39 • AFPAM 63-113 • DAG Chapter 9 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP • DoD Program Protection Plan Outline & Guidance • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
1.2.6	Functional Thread Analysis	Identify the system-level mission critical functions, safety critical functions, and the functions associated with CPI.	• Criticality Analysis, PPP Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 ICD, CDD, and 1.10 Risk Management) • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis & Attack Path Analysis • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.7	Prioritize the Functions	Prioritize the functions based on the user requirements, risk, and intended operational environment (including threats).	• Criticality Analysis, PPP Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 ICD, CDD, and 1.10 Risk Management) • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.8	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. Architect the system boundaries (internal and external) with emphasis on protection of the MCFs, SCFs and functions associated with CPI. **NOTE:** Based on maturity of program, details of the internal and external boundaries may or may not be known.	• Criticality Analysis, PPP Appendix C	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • OSD Trusted Systems and Network Analysis • Appendix A: USAF SSE Acquisition Guidebook (1.1.2 HPT Implementation of JCIDS Survivability KPP and CSAs • Appendix E: Sample PPP • NIST 800-160 3.4.3 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
1.3	**Develop Initial Requirements**				

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
1.3.1	Conduct Criticality Analysis	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.	• Criticality Analysis, PPP Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 Initial Capabilities Document (ICD) and Capability Development Document (CDD), 1.10 Risk Management) • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.2	Conduct Vulnerability Analysis	Analyze inherited vulnerabilities from required system of system connections, including access points and attack paths.	• Vulnerability Analysis • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.2.1	Identify 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 • Cybersecurity risk assessment • MBCRA Input	• SSWG	• DoDI 8500.01 • DoDI 8510.01 • AFI 17-101 • DoD Trusted Systems and Networks (TSN) Analysis • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.2.2	Analyze Entry Access Points and Attack Paths	Analyze cyber Entry Access Points (EAPs) and Attack Paths. Analyze EAPs and Attack Paths 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	• Risk Management Framework for DoD IT Plan • Cybersecurity risk assessment • MBCRA Input	• SSWG • CyWG	• DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Appendix C: Functional Thread Analysis & Attack Path Analysis

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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 a components (hardware, software, and firmware) that could cause the system to fail at some later time.			
1.3.3	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.	• Updated Risk Assessment • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.3.1	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	• Supporting Acq Intel unit • AFOSI	• 10 U.S.C. • DoDI 5000.02 • AFI 99-103 • WBS 1.2.3 (operational environment, deployment locations/scenarios, Acquisition Intelligence Guidebook (AIG)) • NIST SP 800-30 Tasks 1-2 and 1-5 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
			drawings/ DoDAFs • MBCRA Input		
1.3.3.2	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 5000.02 • DoDI 8510.01 • DoDI 8500.01 • AFMAN 14-401 • Acquisition Intelligence Guidebook (AIG) • Appendix E: Sample PPP • NIST SP 800-30 Tasks 1-2 and 1-5
1.3.3.3	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 • MBCRA Input	• SSWG • Supporting Acq Intel unit • AFOSI • Defense Intelligence Agency (DIA) • National Air & Space Intelligence Center (NASIC)	• DoDI 5000.02 • DoDI 8510.01 • DoDI 8500.01 • AFI 63-101/20-101 • AFMAN 14-401 • NIST SP 800-30 • Adversary Cyber Threat Analysis (ACTA) Process • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.3.4	Conduct System Research	Research the system's operation to include its capabilities, functions, external interactions and key dependencies,	• Production Requirements	• Supporting Acq Intel Unit	• DoDI 5000.02, Enclosure 14 • DoDI 8510.01 • DoDI 8500.01

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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.	(PR) Record Copy		• Adversary Cyber Threat Assessment (ACTA) step #15 • Acquisition Intelligence Guidebook (AIG) • NIST SP 800-30 Task 2-4 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.3.5	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 5000.02 • DoDI 8510.01 • DoDI 8500.01 • Adversary Cyber Threat Assessment (ACTA) step #15 • Acquisition Intelligence Guidebook (AIG) • NIST SP 800-30 Task 2-4
1.3.3.6	Translate Intelligence/ Counterintelligence Risk	Use established methodologies to translate Intelligence Community threat rankings to RMF-compatible risk matrices.	• Cyber threat risk matrices	• Supporting Acq Intel Unit • AFOSI	• DoDI 5000.02 • DoDI 8510.01 • DoDI 8500.01 • Adversary Cyber Threat Assessment (ACTA) step #16 • Acquisition Intelligence Guidebook (AIG) • NIST SP 800-30 Task 2-6
1.3.3.7	Deliver Threat Assessment to SSWG	Provide completed forms, associated narrative, and risk transition product to the SSWG.	• Threat Assessment documentation (as required): o Cyber threat risk matrices	• Supporting Acq Intel Unit • AFOSI	• DoDI 5000.02 • DoDI 8510.01 • DoDI 8500.01 • AFI 99-103 • Adversary Cyber Threat Assessment (ACTA) step #16

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
			o Overlays of cyber threats on program design documents o Cyber threat register o Production Center narrative cyber threat analyses o Associated briefings • MBCRA Input		• Acquisition Intelligence Guidebook (AIG) • NIST SP 800-30 Task 2-6 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.4	Unmitigated 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 capture the resultant risk assessment in the MBCRA products.	• Risk Assessment • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.3.5	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	• PPP, Appendix A (SCG)	• SSWG	• DoDM 5200.45 and DoDM 5200.01 V1-V4 • Appendix E: Sample PPP • Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		potential vulnerability information contained in the MBCRA.			
1.3.6	Develop Initial Requirements	Develop initial requirements documents (e.g., 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	• Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specification, 2.3 SOO and SOW, and Attachment 1) • NIST 800-160 3.4.3 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
1.3.6.1	Assess SSE Requirements Implementation	Assess SSE Requirements Implementation using the Excel workbook in Appendix F	• SSE Requirements Implementation Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (Attachment 1) • Appendix F: SSE Requirements Implementation Assessment

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
1.3.7	Perform Requirements Traceability	Trace requirements to appropriate documentation in order to satisfy the AO, TSN, ATEA, and IP.	• Traceability matrix	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.0 Requirements Documents)
1.4	**Categorize System**				
1.4.1	Document Information Types	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 Categorization Document • MBCRA Input	• PM/Information Security Officer (ISO) • Information System Security Manager (ISSM)	• Committee on National Security Systems Instruction (CNSSI) No. 1253, including appendix on overlays • DAG Chapter 9 • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.4.2	Categorize	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 • MBCRA Input	• PM • Information Systems Security Officer (ISSO) • ISSM • AO or designee	• CNSSI No. 1253 • NIST SP 800-37 • Federal Information Processing Standards (FIPS) Publication 199 • DoDI 8500.01 • DoDI 8510.01 • DoDI 5000.02 Enclosure 11 (Clinger-Cohen Act) • Appendix E: Sample PPP • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
1.4.3	Cybersecurity Strategy	Submit the Cybersecurity Strategy (CS) in accordance with the Clinger-Cohen Act. **NOTE:** The Cyber Test Strategy is a component of the CS. The CS should also identify test and evaluation boundaries, resources, etc.	• PPP Appendix E, Cybersecurity Strategy	• PM • ISSO • ISSM • AO or designee • CyWG	• DoDI 5000.02 • AFI 17-101 • AFMAN 17-1402 • CNSSI No. 1253 • NIST SP 800-37 • DoDI 8500.01 • DoDI 8510.01 • Appendix E: Sample PPP
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 SP 800-37 • DoDI 8510.01 • AFI 17-101 • AFI 17-130
1.5	**Develop Draft Program Protection Plan**				
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 and Defense Security Service Threat Assessment).	• PPP Table 5.1-1	• SSWG	• DAG Chapter 7 • DoDI 5000.02 • DoDD 5240.24 • DoDI 5240.04 • AFPAM 63-113 • Appendix E: Sample PPP • Standard Process for Intel Mission Data

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP
1.5.3	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.	• Program Protection Acquisition Strategy Panel (ASP) slide (coordination with ACE) • Risk Register	• PM	• Acquisition Center of Excellence (ACE) • Appendix A: USAF SSE Acquisition Guidebook (1.2.1 Acquisition Strategy Panel (ASP) and 1.10 Risk Management)
1.5.4	Draft Program Documents	Ensure program artifacts include SSE and cyber test considerations.	• Test and Evaluation Master Plan (TEMP) • SEP • Information Support Plan (ISP) • Life Cycle Sustainment Plan (LCSP)	• SSWG • CyWG	• Appendix A: USAF SSE Acquisition Guidebook (1.0 Programmatic Documents) • 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	• 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)) • Appendix E: Sample PPP

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		Management/Information Protection requirements (WBS 1.3) for the program.			
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 & 1.4, as necessary.	• PPP Appendix C • Updated Criticality Analysis • MBCRA Input	• SSWG	• DAG Chapter 9 • Appendix E: Sample PPP • DoDI 5200.44 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.7.2	Review Vulnerability Analysis	Review and update the analysis on WBS 1.3.2 (vulnerabilities from required system of system connections, including access points and attack paths).	• Updated Vulnerability Analysis • MBCRA Input	• SSWG	• DoDI 8500.01 • DoDI 8510.01 • DoD Trusted Systems and Networks (TSN) Analysis • Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.7.3	Review Threat Analysis	Review and update threat analysis initiated in WBS 1.3.3, as necessary. Threat information is based on current intelligence and counterintelligence.	• Updated Risk Assessment • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • 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	• Risk Assessment • SSE Requirements Implementation Assessment • Hazard Assessment	• SSWG • System Safety Group	• DoDI 5000.02 • Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix F: SSE Requirements Implementation Assessment • AFI 91-202 • MIL-STD-882

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		Process. In addition, capture the pairing of threats and vulnerabilities within the MBCRA. Obtain SSE risk 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 mitigate the unapproved risks. Update SSE Requirements Implementation Assessment.	• MBCRA Input		• DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
1.7.4.1	Generate Initial MBCRA Products	Generate MBCRA Report 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 Attack Path Analysis for high risk potential vulnerabilities identified during risk assessment, as needed. **NOTE:** Ensure all resources used, as well as the analysis processes used, assumptions made, and conclusions reached during MBCRA analysis activities are clearly codified in program documents for later reference (particularly during future MBCRA updates). Resources used for MBCRA analysis should be stored in a single resource repository.	• MBCRA Report • MBCRA Data Repository	• CyWG	• DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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. 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	• 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, 1.3, and 1.7, finalize contractor requirements (e.g., SOO/SOW to include CDRLs and DIDs). Ensure requirements are included for necessary test support. Obtain agreement on the requirements from the AO, TSN, ATEA, and IP.	• SOO/SOW or equivalent	• SSWG	• DoDI 5000.02 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW)
2.1.2	Finalize System Requirements	Utilizing WBS 1.2, 1.3, and 1.7, finalize system requirements (e.g., SRD/Spec). Ensure requirements are testable, achievable, and measurable.	• SRD/Spec or equivalent	• SSWG	• DoDI 5000.02 • AFI 99-103

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		Obtain agreement on the requirements from the AO, TSN, ATEA, and IP.			• 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 Section 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)
2.3	**Programmatic Plans**	Develop Information Support Plan (ISP), Life Cycle Sustainment Plan (LCSP), Systems Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP).	• SEP • TEMP • ISP • LCSP	• SSWG • ITT • CyWG	• DoDI 5000.02 • DoDI 8500.01 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (1.7 Information Support Plan (ISP), 1.8 Life Cycle Sustainment Plan

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
					(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	• SSWG • PM • CE • System Safety Group	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix F: SSE Requirements Implementation Assessment • AFI 91-202 • MIL-STD-882 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
	Approve RFP	If approved, then proceed to WBS 3.1. 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

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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 4.1. 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 1.1
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), 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.	• PPP Section 4.0, ATP	• SSWG	• DoDI 5000.02 • DoDI 5200.39 • DoDD 5200.47E • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		ASDB available via SIPRNet at https://www.dodtechipedia.smil.mil/ASDB **NOTE:** Work with the DoD Office of the Executive Agent for Anti-Tamper (ATEA) early and often for guidance.			
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)).	• PPP Section 5.3.6 & Table 5.3.6-1 • SOW • DD Form 254	• SSWG	• WBS 1.3.5 • DAG Chapter 9 • DoDM 5200.01 V1-V4 • DoD 5220.22-M • AFI 31-101 • AFI 63-101/20-101 • Appendix E: Sample PPP
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 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 • 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

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
					Systems Engineering Plan (SEP)) • Appendix E: Sample PPP • Appendix F: SSE Requirements Implementation Assessment
4.2.1	System Requirements Review (SRR)	Conduct SRR per 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 resiliency requirements. Obtain Defense Intelligence Agency – Threat Assessment Center (DIA-TAC) reports for known critical components and evaluate risk to determine proper design. **Prerequisite:** Complete Requirements Analysis in WBS 2.1. If applicable, update requirements analysis in support of SRR.	• SRR Meeting minutes and Action Items • DIA-TAC reports • SSE Requirements Implementation Assessment	• PM • CE • SSWG • CyWG	• DoDI 5000.02 • AFI 99-103 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.2 System Requirements Review (SRR)) • Appendix E: Sample PPP • Appendix F: SSE Requirements Implementation Assessment • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
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	• Architecture Requirements (DoDAF Views)	• SSWG	• DAG Chapter 3, Section 4.2.3. Architecture Design Process • NIST 800-160 3.4.4

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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.			
4.2.3	System Functional Review (SFR)	Conduct SFR per 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 resiliency requirements. In addition, ensure verifiable test requirements are documented. Update system boundaries from WBS 1.2.4.	• 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 C: Functional Thread Analysis & Attack Path Analysis • Appendix F: SSE Requirements Implementation Assessment • IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		Functional Thread Analysis completed for SCFs, MCFs, and CPI. Submit DIA-TAC reports for known critical components and evaluate risk to determine proper design.			
4.2.4	Design / Requirements Decomposition	Complete a decomposition of the architecture and cybersecurity and 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 resilient system.	• System / Subsystem requirements and architecture • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • NIST 800-160 3.4.5 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.5	Preliminary Design Review (PDR)	Conduct PDR per 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 resiliency requirements. Complete an attack path analysis per Section 6 of Appendix C: Functional Thread Analysis & Attack Path Analysis, ensuring boundaries are evaluated. Based on findings, add/modify requirements. Obtain agreement on the security requirements from the AO, TSN, ATEA, 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	• PDR Meeting minutes and Action Items • DIA-TAC reports • Functional Thread Analysis • Updated Risk Assessment • Attack Path Analysis • MBCRA Input • SSE Requirements Implementation Assessment	• PM, CE, SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.4 Preliminary Design Review (PDR)) • Appendix C: Functional Thread Analysis & Attack Path Analysis • Appendix F: SSE Requirements Implementation Assessment • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		document, due to the unique lifecycle of space systems. Submit DIA-TAC reports for known critical components and evaluate risk to determine proper design.			
4.2.6	Finalize Design / Requirements	Finalize the architecture and cybersecurity and 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 • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • NIST 800-160 3.4.5 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.7	Critical Design Review (CDR)	Conduct CDR per 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 resiliency requirements. Update the attack path analysis per Section 6 of Appendix C: Functional Thread Analysis & Attack Path Analysis, ensuring boundaries and identified potential vulnerabilities are evaluated. Based on findings, add/modify requirements and adjust cyber test strategy/scope. Obtain agreement on the requirements from the AO, TSN, ATEA, and IP.	• 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	• PM • CE • SSWG	• 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, Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • Appendix C: Functional Thread Analysis & Attack Path Analysis • Appendix F: SSE Requirements Implementation Assessment • IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		Final Functional Thread Analysis completed for SCFs, MCFs, and CPI. Submit any remaining DIA-TAC reports and evaluate risk to determine proper design.			
4.2.8	Test Readiness Review (TRR)	Conduct TRR per 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. TRRs should be conducted prior to "For Score" testing for Laboratory, Ground and Flight. In 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.	• TRR Meeting minutes and Action Items • Updated Risk Assessment • Test Plans and Procedures • Updated SSE Requirements Implementation Assessment	• PM • CE • SSWG	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 • AFPD 17-1 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.6 Test Readiness Review (TRR)) • Appendix F: SSE Requirements Implementation Assessment • DoD Cybersecurity Test and Evaluation Guidebook
4.2.9	Functional Configuration Audit/System	Conduct FCA/SVR per Appendix A: USAF SSE Acquisition Guidebook Section 4.0.	• FCA/SVR Meeting minutes and Action Items	• PM • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.7 Functional Configuration Audit

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
	Verification Review (FCA/SVR)	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, ATEA, and IP. Submit DIA-TAC reports for any updated critical components and evaluate risk to determine proper design.	• DIA-TAC reports • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment		(FCA) and 4.1.8 System Verification Review (SVR)) • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • Appendix F: SSE Requirements Implementation Assessment
4.2.10	Production Readiness Review (PRR)	Conduct PRR per Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the manufacturing and SCRM processes can support production. Obtain agreement on the requirements from the AO, TSN, ATEA, and IP.	• PRR Meeting minutes and Action Items • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment	• PM • CE • SSWG	• IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.9 Physical Configuration Audit (PRR)) • Appendix F: SSE Requirements Implementation Assessment
4.2.11	Physical Configuration Audit (PCA)	Conduct PCA per 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, ATEA, and IP.	• PCA Meeting minutes and Action Items • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment	• PM • CE • SSWG	• IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.10 Physical Configuration Audit (PCA)) • Appendix F: SSE Requirements Implementation Assessment

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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 5000.39 • DoDI 5000.44 • DoDI 8510.01 • DoDI 8500.01 • AFMAN 14-401 • DoD Trusted Systems and Networks (TSN) Analysis • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix E: Sample PPP
4.3.1	Update Plan of Action and Milestones	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 SP 800-37
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	• DoDM 5200.45 and DoDM 5200.01 V1-V4 • Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems • Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW, Attachment 2 CDRL 42) • Appendix E: Sample PPP • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
4.3.3	Update Programmatic Documents, Monitor protection activities	Update SEP, TEMP, and LCSP. 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.	• 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 • 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 E: Sample PPP • DoD Program Protection Plan Outline & Guidance
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. Update SSE Requirements Implementation Assessment.	• Updated Risk Assessment • SSE Requirements Implementation Assessment • Hazard Assessment	• SSWG • PM • CE • System Safety Group	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix F: SSE Requirements Implementation Assessment • AFI 91-202 • MIL-STD-882

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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.			• (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
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. See DoDI 5000.02 Enclosure 2, paragraph 2.	• PPP	• SSWG • PM • MDA • PEO	• DoDI 5000.02 • AFI 63-101/20-101 • AFPAM 63-113 • DAG Chapter 9 • OSD PPP Outline and Guidance, PPP example, and OSD Evaluation Criteria • Appendix E: Sample PPP
	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 • 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)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
					• AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
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
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 SP 800-37 • AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
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 to 4.2.9). Update test plans, as necessary. Ensure test plan(s) match the test strategy outlined in the CS and TEMP.	• Updated test plans, TEMP	• SSWG • CyWG	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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 • CVI test report(s) • MBCRA Input • Updated cyber test portions of CS and TEMP • Vulnerability Reports • ACD test report(s) • DT&E artifacts	• SSWG • CyWG	• DoDI 5000.02 Enclosure 4 • 10 U.S.C. • 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	• Updated Risk Assessment • CVI test report(s) • MBCRA Input • Updated cyber test portions of CS and TEMP	• SSWG • CyWG	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 3)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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 activities conducted to date. Update requirements as necessary. **NOTE:** Vulnerability 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.			
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 penetration testing with the intent of causing mission effects.	• Vulnerability Report • ACD test report(s) • MBCRA Input • DT&E artifacts • Updated cyber test portions of CS and TEMP	• SSWG • CyWG	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 4)

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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)	• SSWG • CyWG	• DAG Chap 8- 3.2 Operational T&E • 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 5 and 6)
5.2.3.1	Cooperative Vulnerability and Penetration Assessment (CVPA)	Conduct a Cooperative Vulnerability and Penetration Assessment. The OTA completes a CVPA either before or following MS C, as appropriate. The purpose is to provide a comprehensive characterization of the cybersecurity and resiliency status of a system in an operationally representative context. Also identify any additional cyber vulnerabilities introduced by new interfaces and the operational system-of-systems environment. **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	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 5) • 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	• Test and Evaluation Reports	• SSWG • CyWG	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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	• AA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required)		• AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 6) • DOT&E Memo: Procedures for Operational Test & Evaluation of Cybersecurity in Acquisition Programs
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. For each vulnerability identified, conduct risk assessment in WBS 4.4. Capture any vulnerabilities or deficiencies in Joint Deficiency Reporting System (JDRS). Deficiencies should be linked to requirements.	• DT&E and OT&E reports • MBCRA Input • Updated cyber test portions of the CS and TEMP (if required)	• SSWG • CyWG	• 10 U.S.C. • DoDD 5000.01 • DoDI 5000.02 • AFI 99-103 Section 5.19, 5.20 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		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 • (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) • Appendix E: Sample PPP
6.3	**Monitoring**	Determine the security impact of proposed or actual changes to the system, environment, threats, and vulnerabilities.	• POA&M • PPP Section 9.1 & Appendix E (Cybersecurity Strategy)	• PM	• NIST SP 800-37 • AFPAM 63-113 • NIST SP 800-137 • Appendix E: Sample PPP
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	• NIST SP 800-37

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
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 SP 800-37
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 SP 800-37 • Appendix E: Sample PPP
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 SP 800-37 • Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP)) • Appendix E: Sample PPP
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); 2.3.1 Program Protection) • Appendix E: Sample PPP
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 • Appendix B: USAF Combined CPI/CC Identification Guide • Appendix E: Sample PPP
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 • Appendix E: Sample PPP
6.3.8	Deficiency Reporting	Review Deficiency Reports (DRs) and complete root cause analysis reporting as necessary.	• DR • Updated risk assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.3.1 Program Protection) • Air Force Cyber Resiliency Office for Weapon Systems

WBS	Activity	Description	Artifact	OPR/ Supplier	Tool/Traceability
		NOTE: Upon an incident and/or deficiency, update risk assessment.			(CROWS) Cyber Incident Coordination Cell (CICC) and Cyber Incident Response Team (IRT) for Weapon Systems Concept of Operations
6.3.9	Continuous Monitoring	Continuously monitor cybersecurity and 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 16 per Appendix A: USAF SSE Acquisition Guidebook (2.3.2 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, 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	• 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
End					

5.0 SSE Requirements Implementation Assessment.

5.1 During the design and development of a new weapon system, or modification to an existing weapon system, an assessment of how cybersecurity and 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).

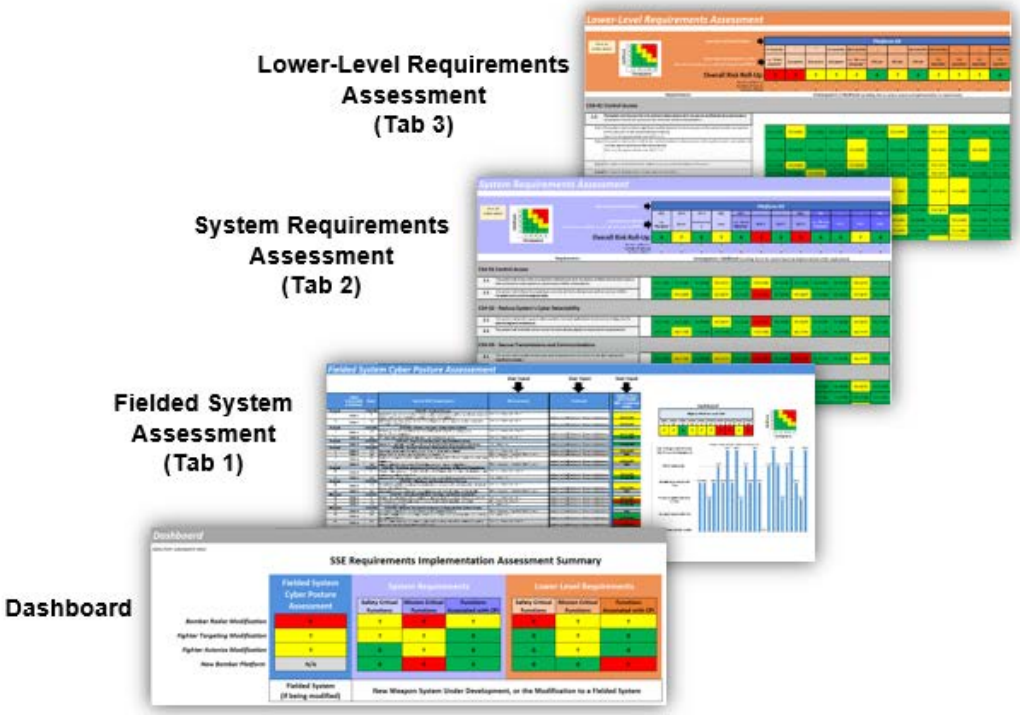


FIGURE 12: SSE Requirements Implementation Assessment Tool.

6.0 Roles and Responsibilities.

6.1 Overview.

6.1.1 Detailed responsibilities for key Program Protection Planning tasks can be found within the WBS table, located in Section 4.4 of this document.

6.2 Program Manager.

6.2.1 Conducts Program Protection Planning activities and prepares a PPP IAW this guide.

6.2.2 Ensures Cybersecurity and Resilience requirements, attributes, and design consideration are designed into newly acquired systems and modified systems.

6.2.3 Appoints a Program Protection Lead to coordinate and execute security related tasks and facilitate the SSWG.

6.2.4 Ensures the PPP and annexes are reviewed and coordinated with the appropriate stakeholders.

6.2.4.1 Submits the PPP to the MDA for approval

6.2.4.2 The Cybersecurity and Resiliency Appendices will be coordinated and reviewed by the respective Authorizing Official (AO) or designated representatives.

6.3 Systems Engineer.

6.3.1 Ensures the development and delivery of cyber resilient capability through the implementation of SE balancing system cost, schedule, performance and risk (ensure based on threats and vulnerabilities).

6.4 Systems Security Engineer.

6.4.1 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, sections 2.0 and 3.0.

6.4.2 Ensures SSE Requirements to satisfy protection needs are implemented through the SE process and tested through the program office's test program.

6.4.3 Ensures security approaches are documented in the PPP.

6.4.4 Ensures PPP remains current and informed by the SE reviews, constraints and decisions. Ensure emerging threats are continually assessed and incorporated in requirements/design.

6.4.5 Conducts and leads program protection analyses for program and system information, CPI, and critical components.

6.5 Local Intelligence Lead.

6.5.1 Ensures intelligence analysis, to include assessment of the intelligence mission data requirements, supports Program Protection Planning objectives.

6.6 Air Force Office Of Special Investigations (AFOSI).

6.6.1 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

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

6.7.1 Collaborate with the systems security engineer in order to inform the program protection analyses and modify the security protection measures to meet program needs.

6.7.2 Identify security vulnerabilities and needed security protection measures within the scope of their expertise.

6.7.3 Define, implement and monitor security protection measures, and additional security requirements (i.e. awareness training, reporting, etc.).

6.8 Process Owner (Local systems engineering office).

6.8.1 Reviews PPP sent up the chain to SAF/AQ and DoD.

6.8.2 Maintains and coordinates changes to this process.

6.8.3 Leads process improvement and change events related to this process.

6.8.4 Assists Program Offices with PPP development and coordination.

6.8.5 Provides training upon request.

6.9 Milestone Decision Authority/Program Executive Officer.

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

6.10 Systems Security Working Group (SSWG).

6.10.1 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), and representatives from the Cyber Working Group (CyWG), AO, TSN, ATEA, and IP.

6.10.2 Gathers documentation to assist with the review and understanding of what the customer requirements, capabilities, and desired effects are.

6.10.3 Facilitates and ensures the completion of the Program Protection Analysis, Criticality Analysis, Initial Attack Path Analysis, Requirements Analysis and reviews results.

6.10.4 Facilitates and ensures the completion of the Threat Assessment, Vulnerability Assessment, Risk Assessment and reviews results.

6.10.5 Facilitates, reviews, and ensures the development of the PPP and security plans per DoDI 8500.01 and DoDI 8510.01.

6.10.6 Identifies required clauses (FAR, DFARS, AFFARS) in conjunction with Procuring Contracting Officer.

6.11 Key Stakeholders (AO, TSN, ATEA, and IP).

6.11.1 See WBS for responsibilities.

7.0 Tools and Training.

7.1 Appendix A: USAF SSE Acquisition Guidebook.

7.2 Appendix B: USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components Identification.

7.3 Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems

https://www.dtic.mil/DTICOnline/home.search

7.4 DoD Cybersecurity Test and Evaluation Guidebook 25 April 2018 Version 2.0.

https://www.dau.edu/tools/t/DoD-Cybersecurity-Test-and-Evaluation-Guidebook

7.5 PM Toolkit.

https://hanscomnet.hanscom.af.mil/pmtb/MR/MR.html.

7.6 National Institute of Standards and Technology Special Publication Website https://www.nist.gov/publications

7.7 Systems Engineering DAU courses.

http://icatalog.dau.e/onlinecatalog/tabnav.aspx

7.8 Committee on National Security Systems library of publications:

https://www.cnss.gov/CNSS/searchForm.cfm

7.9 E-Publishing website for Air Force instructions and publications:

https://www.e-publishing.af.mil/Product-Index/

7.10 For AFLCMC programs: AFLCMC Standard Process for Assessment and Authorization.

https://cs2.eis.af.mil/sites/21710/gov/APDSP/Forms/AllItems.aspx

7.11 There are multiple venues to receive Program Protection Training depending on the level of detail required.

7.11.1 AFLCMC hosts a 3-Day Program Protection Training class, available quarterly, with a Distance Learning option available during the course. Courses dates and links to the course can be reached here: https://www.milsuite.mil/book/groups/acquisition-program-protection-planning.

7.11.2 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

8.0 References to Law, Policy, Instructions or Guidance.

TABLE 3: Key References

Number	Title
AFI 17-101	Risk Management Framework (RMF) for AF Information Technology
AFI 17-130	Air Force Cybersecurity Program Management
AFI 63-101/20-101	Integrated Life Cycle Management
AFI 99-103	Capabilities-Based Test and Evaluation
AFPAM 63-113	Protection Planning for Life Cycle Management
AFMAN 14-401	Intelligence Analysis and Targeting Tradecraft / Data Standards
AFMAN 17-1402	Air Force Clinger-Cohen Act (CCA) Compliance Guide
AFMAN 63-119	Certification of System Readiness for Dedicated Operational Testing
AFMCI 63-1201	Implementing operational safety, suitability and effectiveness (OSS&E) and life cycle systems engineering (LCSE)
CNSSI 1253	Security Categorization and Control Selection for National Security Systems

AF/A5R Requirements Development Guidebook, Volume 4 Air Force Procedures: Modification Proposals (use of AF Form 1067)	Section 2. Guidance for Modifications and use of AF Form 1067
Cyber Survivability Endorsement Implementation Guide v 1.0.1	Joint Chiefs of Staff Cyber Survivability Endorsement Implementation Guide
Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems	Cybersecurity Classification/Declassification Guide for Air Force Weapon Systems is available at: https://www.dtic.mil/DTICOnline/home.search
Defense Acquisition Guidebook Chapters 3, 7, 8 and 9	Chapter 3: Systems Engineering Chapter 7: Intelligence Support & Acquisition Chapter 8: Test and Evaluation Chapter 9: Program Protection
DoD 5220.22-M	National Industrial Security Program Operation manual
DoDD 5200.47E	Responsibilities for Anti-Tamper (AT) protection of (CPI)
DoDD 5240.24	Counterintelligence Activities Supporting Research, Development, and Acquisition
DoDD 5000.01	The Defense Acquisition System
DoDI 5000.02	Operation of the Defense Acquisition System
DoDI 5200.39	Critical Program Information (CPI) Protection Within the DoD
DoDI 5200.44	Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
DoDI 5240.04	Counterintelligence Investigations
DoDM 5200.45	Procedures for Developing Security Classification Guides
DoDI 8500.01	Cybersecurity
DoDI 8510.01	Risk Management Framework (RMF) for DoD IT
DOT&E TEMP Guidebook	Office of the Director, Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) Guidebook
IEEE 15288.2	Standards for Technical Reviews and Audits on Defense Programs

MIL-HDBK-520	Systems Requirements Document (SRD) Guidance
MIL-STD-882E	DoD Standard Practice – System Safety
NIST Special Publication 800-30	Guide for Conducting Risk Assessments
NIST Special Publication 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems
NIST Special Publication 800-53	Security and Privacy Controls for Information Systems and Organizations
NIST Special Publication 800-160	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
Trusted Systems and Networks (TSN) Analysis	Trusted Systems and Networks (TSN) Analysis published by the Deputy Assistant Secretary of Defense for Systems Engineering and the Department of Defense Chief Information Officer
Security Management/Information Protection	Contact local security manager for more information
United States Code (U.S.C) 10	United States Code - Title 10: Armed Forces

APPENDIX A – USAF Systems Security Engineering (SSE) Acquisition Guidebook

Version 2.0

12 March 2020

APPENDIX A

FOREWORD

Comments, suggestions, or questions on this document should be captured in the Comments Resolution Matrix (CRM), found in Appendix K, and emailed to the Cyber Resiliency Office for Weapon Systems (CROWS@us.af.mil).

RECORD OF CHANGES

Version	Effective Date	Summary
2.0	12 Mar 2020	Added supplemental text to link the Functional Thread Analysis (FTA) references to the new Appendix C, which further explains the FTA process, removed Capability Production Document (CPD) references throughout in line with newest JCIDS policy, tailored the SOO/SOW sample contract language with updates from National Defense Industrial Association (NDIA) Systems Security Engineering Committee, added Controlled Unclassified Information (CUI) SOO/SOW paragraph, updated Systems Engineering Technical Review (SETR) SSE Entry Criteria tables for FTA changes, renamed the “Criticality Analysis” CDRL to “FTA” (CDRL# 20) and split contractor Security Plan CDRL #15 into CDRL #15 (Development Environment) and #16 (Weapon System) in the CDRL table in Attachment 2, revised the SOO/SOW Requirements Trace table in Attachment 3.
1.4.1	14 Jan 2019	Section 3.2 – Section L changed DoDI reference typo. Updated contract language sections to expand to both clauses and provisions. Corrected four provisions that were misidentified as clauses.
1.4	21 Sep 2018	Added Acquisition Strategy Plan information to section 1.2.1. Added Attachment 1 with detailed system SSE requirements listing embedded within, and updated Sections 2.2 and 2.3 with related contractor SSE requirements. Updated the CDRL table in Attachment B in order to capture all cybersecurity and resiliency requirements. Updated Table 2.2-1. Updated entry criteria for SETRs in Section 4.0 in order to match and trace the updates to Section 2.
1.3	8 May 2018	Significantly reduced and streamlined the Statement of Work and Statement of Objective sections and combined in to one section, Section 2.3. Simplified and combined Section 2.2, System Specification and Section 2.4, System Requirements Document into one section, Section 2.2. Updated the DFARS clauses in section 3.1 and reviewed applicability of all. Also included a preamble in Section 3.1 pointing the reader to their Procuring Contracting Officer (PCO) to verify all applicable clauses. Updated and streamlined the Systems Engineering Plan Section 1.12. Significantly revised and bolstered the Risk Management,

		Section 1.10. Updated Section 5 (now Section 4) with revised SETR entry/exit criteria tables, and mapped each to the new SOW section paragraphs. Removed entire Section 4 on CDRL language, condensed CDRL and DID info into the SOW section, and expanded the CDRL/DID table in Appendix A. There is still some work to finish to map every SOW requirement listed to the appropriate DID number. Condensed all of Sections 3.2 and 3.3 Sections L & M examples into simplified RFP guidance in line with AFLCMC Acquisition Center of Excellence feedback on RFP best practices. Removed Software Acquisition Management Plan (SWAMP) section as it is not a required document. Added Section 2.2.1, referencing cyber hygiene.
1.2	30 Aug 2017	Updated and revised entire document. Added multiple sections. Included recent policy & guidance updates: DoDI 5000.02, DAG Chapter 9, AF 17-Series policy documents, FAR/DFARS/AFFARS, ASSIST database for DIDs, DoD AT Desk Reference, and others as identified. Added, deleted, and/or updated definitions, references, and acronyms. Added section for Cybersecurity Strategy. Reviewed revised acquisition document templates and updated sections for AS, ISP, LCSP, RMP, SEP, and TEMP. Updated PWS, Specifications, SOO & SRD sections by adding templates and example statements. Reviewed and updated FAR/DFARS/AFFARS. Aligned/updated SOW language to reflect DAG Chapter 9 changes: Program Protection, AT, Cybersecurity, Exportability Features, HwA, SwA and SCRM. Reviewed ASSIST database and updated/added CDRLs & DIDs. Sorted CDRLs according to DAG Chapter 9/SOW functional areas (see above). General editing and formatting for consistency.
1.1	24 Mar 2017	Updated definitions and reconciled with the Cyber Campaign Plan (CCP) Lexicon. Incorporated Initial Capabilities Document, Capability Development Document, and Capability Production Document guidance consistent with Cyber Survivability. Endorsement Implementation Guide. Made administrative changes. Submitted to CROWS on 24 March 2017.
1.0	16 Dec 2016	Basic document. Submitted to Cyber Resiliency Office for Weapon Systems (CROWS) on 16 December 2016.

TABLE OF CONTENTS

Executive Summary.

This guidebook 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 AF weapon 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:

- 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.

To emphasize, SSE utilizes SE to bake in Program Protection requirements which account for Cybersecurity, Cyber Resiliency, and Cyber Survivability. The policies referenced in this document are listed in Table 1.

TABLE 1: Referenced Policies.

Number	Title	Description
DoDI 5000.02	"Operation of the Defense Acquisition System"	• DT&E cybersecurity assessment requirements • Cybersecurity assessments to occur at Milestones
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
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 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
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
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]

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 [1], 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, 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. **It should not be used to "cut and paste" without understanding its applicability to the program. Thus, language in each section may need to be modified to meet the specific needs of the PO.**

[1] 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.

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 Initial Capabilities Document (ICD) and Capability Development Document (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 ICD, 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 weapon system requirements, including those that account for SSE activities throughout the acquisition life cycle. When drafting the ICD or CDD the using Command, with input from the PO, must take into account SSE-related capabilities.

1.1.1 ICD/CDD – System Survivability (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 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 ICD/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 Analysis of Alternatives (AoA), ICD and 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/.

For cyber, 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 can be viewed as the realization of these three pillars.

Additionally, each pillar has associated Cyber Survivability Attributes (CSAs) that must be considered for incorporation into all capability requirement documents:

TABLE 1.1.1-1: Cyber Survivability Attributes.

	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 Counter Vulnerabilities at Tactically Relevant Speeds

The CSEIG includes a process to determine the strength of CSA for the ICD and 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).

JCS CSEIG Recommended Cyber Survivability ICD Language.
The following is an EXAMPLE of ICD language from the CSEIG. In many cases, this can be used directly for the 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 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 AoA alternative and tailored for system-specific architectures are:*

1. *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.*
2. *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.*
3. *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.

JCS CSEIG Recommended Cyber Survivability 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.*

JCS CSEIG Recommended Cyber Survivability CDD Language.
The expectation for the 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 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.*

The following is recommended language for the creation of system attributes to implement the CSAs. The following language assumes that the weapon system is considered “Very High” with respect to the Cyber Survivability Risk Category (CSRC). If the associated 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.*
  - *The system takes active measures to identify and deny unauthorized access attempts, to include Denial of Service (DOS) and Distributed DOS (DDoS), at the system, its internal partition boundaries, and system interfaces with other systems.*
- **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 and 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 Counter Vulnerabilities at Tactically Relevant Speeds.**
  - *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.*

1.1.2 High-Performance Team (HPT) implementation of the JCIDS Survivability KPP and Cyber Survivability Attributes (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 ICD to 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 ICDs and/or CDDs for the Survivability KPP and CSAs, the SSWG should follow the Functional Thread Analysis process / methodology in Figure 1.1.2-1 is recommended to ensure the requirements are allocated appropriately. 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 ICD/CDD to the detail design requirements documented in the System Requirements Document (SRD) and System Specifications. See section 2.2 of this document for more information on the System Requirements Document and System Specification. For more information on the Functional Thread Analysis, see Appendix C.

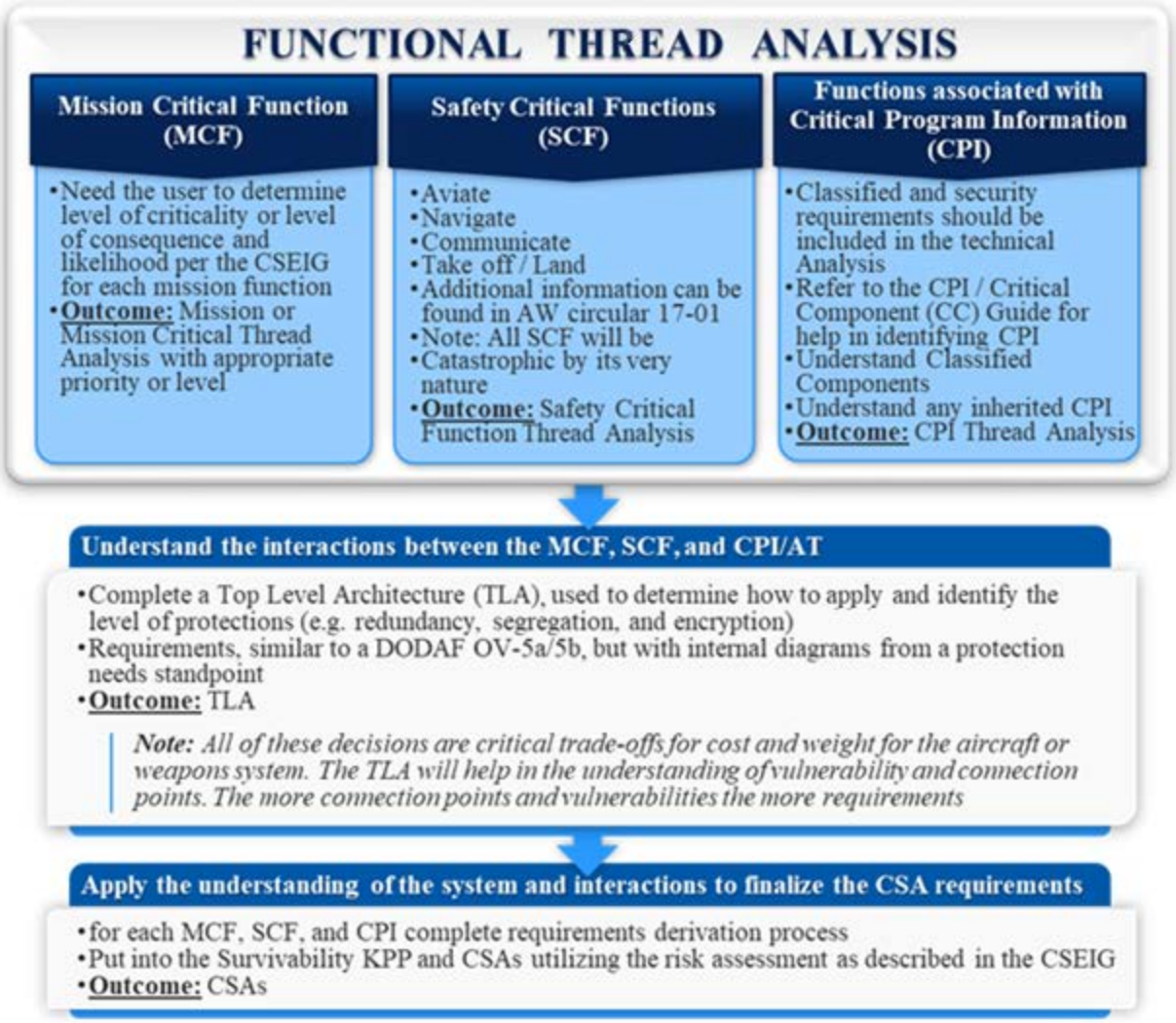


FIGURE 1.1.2-1. CSA Requirements Allocation.

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 current policies mentioned in the Background and Section 4.2.1 of the main document. It is important to understand that Cyber Resiliency cannot be obtained or maintained without Cybersecurity.

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 1.1.2-2.

FIGURE 1.1.2-2. Cyber Survivability Pyramid.

1.2 Acquisition Strategy (AS).

The AS[2] is developed by the 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.).

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

- **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.

- **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 assessments, 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 (ASP).

The 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 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 resiliency considerations are incorporated into the acquisition strategy. The following is the recommended Cybersecurity and Resiliency chart to include in the technical portion of the ASP briefing.

- Has the program completed a Criticality Analysis 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?

TABLE 1.2.1-1: Cybersecurity and Resiliency ASP Chart.

Cybersecurity and Resiliency	Authority and Date concurrence	SRD/ Spec	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						

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 shall populate the ASP chart, and the PM, Director of Engineering (DOE), and Chief Engineer (CE) approve the content of the 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.

1. 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 ATEA's name and date would be annotated).
2. 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.

3. 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 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:

    2.1 Performance Work Statement (PWS).
    2.2 System Requirements Document (SRD) and System Specifications.
    2.3 Statement of Objectives (SOO) and Statement of Work (SOW).
    3.1 Request for Proposal (RFP) – Contract Clauses (NOTE: sections 3.1.1, 3.1.2, and 3.1.3 contain the specifics on recommended lists of FAR, DFARS, and AFFARS Clauses).
    3.2 Request for Proposal (RFP) – Section L.
    3.3 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.

4. 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 AG.
    - Yellow – The Authority has not approved the RFP/Solicitation, but the program has sufficient rationale to proceed. (Recommend rationale be put in notes section of slide).
    - Red – No cyber language is in the RFP per Appendix A: SSE AG (Recommend rationale be put in notes section of slide).

Additional applicable SSE policy and guidance: DoDI 5000.02, 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:

1. The Government desires new and creative solutions to problem statements.
2. Using a conventional SOW could result in unintentionally stifling ideas and concepts given many possible approaches.
3. 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.
4. The Government must be able to state its objectives in terms of areas of need or interest rather than specific solutions or outcomes.
5. Meaningful proposals with varying technical/scientific approaches are reasonably anticipated.
6. 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.*
- *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 5000.02 (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, Security Plan for Risk Management Framework.*

  The SAF/CIO A6XA CCA Point of Contact can be contacted directly or through the CCA Workflow box usaf.pentagon.saf-cio-a6.mbx.af-cio-clinger-cohen-compliance@mail.mil. The Defense Acquisition Guidebook https://dag.dau.mil/Pages/Default.aspx and the USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site https://cs2.eis.af.mil/sites/10774/default.aspx contain authoritative sources, information, and templates to aid in preparing a CCA compliance package and in learning about DoDI 5000.02 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.*
- **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 Initial Capability Document (ICD) and Capability*

Development Document (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. 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 Interface Control Documents (ICDs). Identify the SSE milestones, to include cybersecurity, as reflected in the program enterprise master schedule (EMS) and integrated master schedule (IMS).*
- **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 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.*
- **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, AT Executive Agent (ATEA), 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. If applicable, SSE considerations are included in the ISP in the following section(s):

- **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. For most ISPs, this will be Distribution Statement D. Be sure to include any applicable SSE-related handling, disposal, and destruction notices.*
- **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)* [3] *, 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 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 (COIs) and the COI 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*

[3] Additional details provided at the AF Interoperability/Information Support Plan SharePoint page https://cs3.eis.af.mil/sites/OO-AQ-AF-18/default.aspx.

(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 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 (www.esi.mil).*
- **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.).*

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 LSCP is required at the Production Readiness Review (PRR) for full-rate production. Refer to DoDI 5000.02 for more information on these delivery requirements.
If applicable, 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, 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 data, sub-system 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 than 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 if any SSE-related requirements have created 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 weapon systems or subsystems that are part of the platform.*
- **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.).*
- **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 PO and is the single source used to coordinate and integrate all protection efforts. 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 2.2-1.*
- **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 or final ATP must be completed. Describe plans for engaging with the respective Government AT Lead and, the ATEA.*
- **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 1.9-1: Sample Table for Application of Software Assurance Countermeasures.

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							

(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 https://ac.cto.mil/wp-content/uploads/2019/06/SwA-CM-in-PPP.pdf)

- **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).*
- **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 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 resiliency risks at the same time and in the same format as programmatic (cost/schedule/performance) risks.

Cybersecurity and 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.

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.

The content below has been derived from NIST SP 800-30, 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 1.10-1: Risk Management Process Step.

Risk Management Process Step	Instructions
Risk Management Planning	AFI 63-101/20-101, AFPAM 63-128, DoD RIO Guide, and additional considerations from this guidance.
Risk Identification	This document
Risk Assessment - Likelihood	This document
Risk Assessment - Consequence	This document
Risk Assessment - Risk	AFI 63-101/20-101, AFPAM 63-128, and DoD RIO Guide
Risk Handling Planning & Implementation	AFI 63-101/20-101, AFPAM 63-128, and DoD RIO Guide
Risk Tracking	AFI 63-101/20-101, AFPAM 63-128, and DoD RIO Guide

A note on System Safety Risks: 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 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, *Translation of MIL-STD-882 Risk Matrix to the OSD Risk Management Guide Matrix.*

- **Cybersecurity and Resiliency process for risk management planning.** Include a description of how system security risks will be managed in program risk management plans IAW 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:

TABLE 1.10-2: SSE Considerations for the Program's Risk Management Plan.

• 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, ATEA, 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 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, ATEA, 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 & Attack Path Analysis. Potential sources of risk include, but are not limited to:

TABLE 1.10-3: 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
System interfaces	- All network and system interfaces - Adversary exploiting penetrations of the 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 - 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) separately for determining Anti-Tamper consequence of compromise.

- **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. This data comes from threat and vulnerability assessments.
  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. This data comes from threat and vulnerability assessments.

TABLE 1.10-4: Likelihood of Threat Occurrence.

Likelihood of Threat Occurrence	
AFPAM 63-128	Tailored version of NIST SP 800-30 Table E-4, *Relevance of Threat Events* and DoD Risk Assessment Guide Table 2-*10 Likelihood of Threat Event Initiation (Adversarial) or Occurrence (Non-Adversarial)*
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 1.10-5: Likelihood of Threat Success.

Likelihood of Threat Success	
AFPAM 63-128	Tailored combination of NIST SP 800-30, Table D-3, *Characteristics of Adversary Capability* and NIST SP 800-30, Table G-4, *Likelihood of Threat Events Resulting in Adverse Impacts*
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%).

Combining the two factors of Likelihood of Threat Occurrence from Table 1.10.4 and Likelihood of Threat Success from Table 1.10.5 (reference NIST SP 800-30, Table G-5) results in the system security risk likelihood factor for LCRM analysis, i.e., the "likelihood" as shown in Table 1.10-6.

TABLE 1.10-6: Risk Likelihood.

Likelihood						
Likelihood of Threat Occurrence (see 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 (see 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 1.10-7: Vulnerability Severity.

Vulnerability Severity	
AFPAM 63-128 Tailored	AFLCMC Standard Process for Cybersecurity A&A, Table 4, which is highly tailored from NIST SP 800-30, Table F-2.
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 1.10-8: Mission Criticality.

Mission Criticality	
AFPAM 63-128 Tailored	Combining Protection Failure Criticality Levels for DAG, Chapter 9, Table 3, and TSN Analysis (June 2014), Table 2-1, with information classification level verbiage.
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.

Combining the two factors of Vulnerability Severity and Mission Criticality using NIST SP 800-30, Table G-5 results in the system security risk consequence factor for LCRM analysis as shown in Table 1.10-9.

TABLE 1.10-9: Risk Consequence.

Consequence						
Vulnerability Severity (see 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 (see 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 1.10-10: 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				

- **Risk Tracking.** IAW AFPAM 63-128 and AFI 63-101/20-101.

NOTE: Security risk must be marked, stored and handled IAW the security classification guide of the program.

Worked Example: Figure 1.10-11 graphically shows how to flow through the system security risk assessment step of the risk management process.

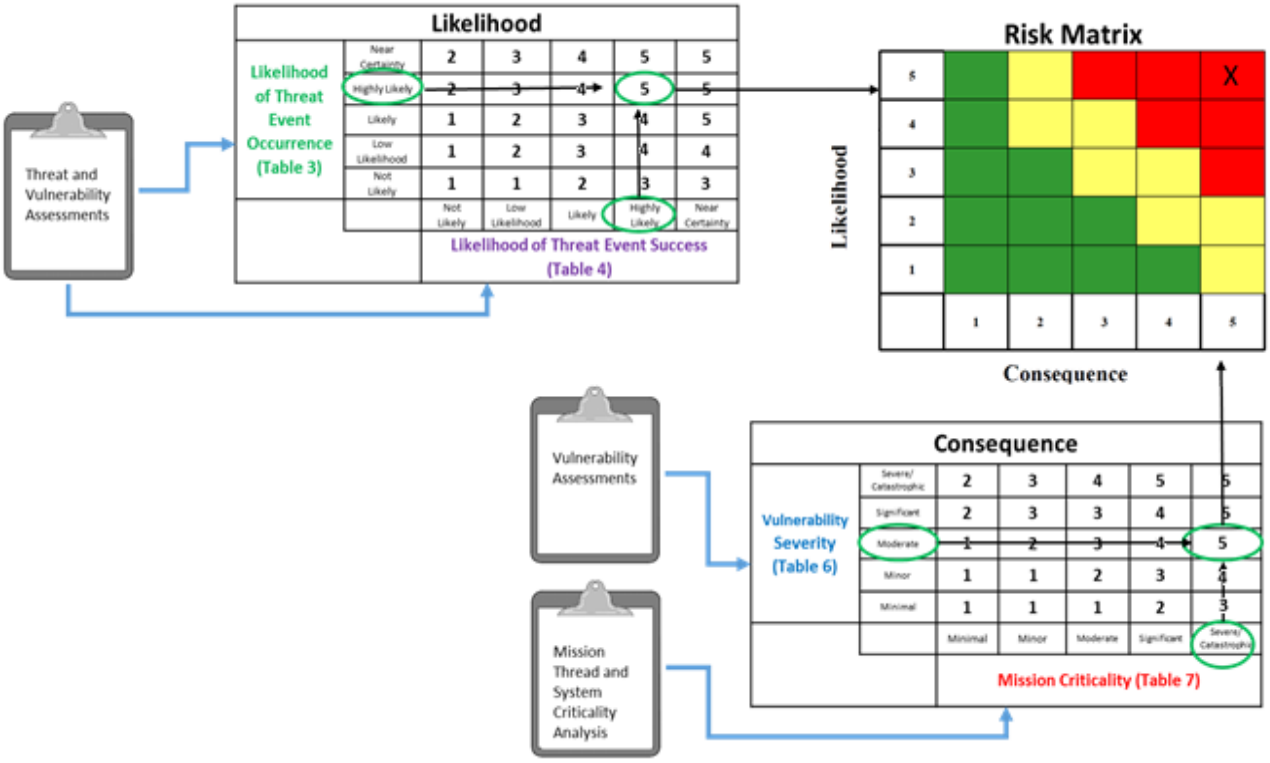


FIGURE 1.10-11: Risk Assessment Example.

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 1.11-1 when planning SSE activities for the program.

TABLE 1.11-1: Factors to Consider When Planning SSE Activities.

• 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

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 architecture 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 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 assessments, 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. 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, ATEA, 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 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 Verification Matrix (RVM), Risk Management Information System (RMIS), etc.). Include in Table 4.7-1, Engineering Tools.*
- **Annex A "Acronyms."** – *Include any SSE-related acronyms.*

1.12 Test and Evaluation Master Plan (TEMP).

The TEMP is prepared by the PO and describes the concept for T&E throughout the program life cycle. It starts with Technology Development (TD) and continuing through Engineering, Manufacturing and Development (EMD) into the Production and Deployment (PD) Phase. The TEMP is submitted for approval prior to Milestone A. TEMP updates are required at the Development RFP Release decision, Milestone B, Milestone C, and full-rate production (FRP)/Fielding Decision (FD). Development of a TEMP will require early involvement of SSE-related testers, evaluators, and assessors as a program conducts pre-system acquisition activities. These personnel will provide the necessary SSE-related technical, operational, and programmatic expertise to ensure security requirements are verified through the appropriate means – demonstration, inspection, analysis, and test. If applicable, include SSE considerations in the following TEMP section(s):

- **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, 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."** – *Include SSE-related verification considerations in the overall evaluation approach focusing on key SCRM decisions and addressing key SSE-related system risks and issues. Evaluation should encompass prevent, mitigate and recover cyber defense functions.*
- **Section 3.3, "Developmental Test Approach."** – *Include the SSE-related approach to test the system performance in a mission context. 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.*
- **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)."** – *Include any SSE-related considerations to ensure the system will be certified safe and ready for IOT&E, such as completion of any SSE-related assessments (e.g., cybersecurity, 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."** – *Describe the overall strategy for evaluation of SSE in support of mission accomplishment, suitability, and survivability. Define cybersecurity measures for prevent, mitigate and recover. 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."** – *Identify the key SSE-related operational test objectives for each test event and test phase. Identify when the CVPAs and*

adversarial assessments (AAs) will be conducted. For each test, include an SSE-related test architecture with test boundary identifying which systems are to be included and excluded from each test.

- **Section 3.5.1.1, "Cooperative Vulnerability and Penetration Assessment."** – *Define the SSE-related data collection methods (i.e., automated scanning/exploitation tools, physical inspection, document reviews, and personnel interviews). Identify all SSE-related data and metrics to be collected.*
- **Section 3.5.1.2, "Adversarial Assessment."** – *Identify the NSA-certified and United States Cyber Command (USCYBERCOM)-accredited team that will execute the AA cyber activities for the OTA. 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. 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 3.5.1.4, "Cybersecurity Test Architecture."** – *Include a detailed, SSE-relevant diagram indicating which elements are included (inside the test boundary) or excluded from the test (e.g., major subsystems, all connections including their protocols, all physical access points, etc.).*
- **Section 3.5.2, "Operational Evaluation Framework."** – *Include the SSE-related goals of the operational test within a mission context. Identify planned sources of SSE-related information (e.g., developmental testing, testing of related systems, modeling, simulation, etc.).*
- **Section 3.5.2.1, "Cybersecurity Critical Issues."** – *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 (e, g, classification issues, threat realism, resource availability, limited operational environments, limited support environment, maturity of tested systems or subsystems, etc.).*
- **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 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 (WBS).

A WBS (see MIL-STD-881) 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 Section 2.3, Statement of Objectives (SOO) and Statement of Work (SOW) of this document.

2.0 Requirements Documents.

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

2.1 Performance Work Statement (PWS).

A 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 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?

EXAMPLE SSE PWS Task Statements.

The contractor shall:

- *Analyze the system architecture and define the system security baseline.*
- *Capture, collate, and report SSE-related risks, opportunities, and issues for the <Insert SYSTEM NAME>.*
- *Conduct SSE-related system, subsystem, and component vulnerability and risk assessments.*
- *Develop and analyze SSE-related program risks and mitigations.*
- *Develop and recommend SSE-related process improvements.*
- *Evaluate, participate, and prepare status of SSE-related aspects of Program Management Review (PMR), Integrated Baseline Review (IBR), technical reviews, and audits.*
- *Identify, maintain, and manage SSE-related deficiency documentation.*
- *Oversee prime contractor and subcontractor SSE-related performance.*
- *Plan, develop, and maintain SSE-related capabilities and operational concepts.*
- *Plan, track, and schedule SSE-related milestones.*
- *Prepare and maintain SSE-related operating instructions for the <Insert SYSTEM NAME>.*
- *Provide SSE management support for the <Insert SYSTEM NAME>.*
- *Support SSE-related system integration, test planning, and test execution for the <Insert SYSTEM NAME>.*
- *Support SSE activities for the <Insert SYSTEM NAME>.*

2.2 System Requirements Document (SRD) and System Specifications.

The SRD consists of system-level requirements that have been derived from user capability requirements documented in the ICD, 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 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 specifications from the following documents:

- Cybersecurity through National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls per DoDI 8500.01 and DoDI 8510.01 as agreed by the Authorizing Official.
  - To include Trusted Systems and Networks (TSN) per DoDI 5200.44.
- Anti-Tamper (AT) Plan per DoDI 5200.39 and 5200.47 as agreed by the ATEA.
- Cyber Resiliency per the user documentation (Initial Capability Document (ICD), Capability Development Document (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 Section 1.1 for the JCIDs requirements to meet the System Survivability KPP and CSAs. Section 1.1.2 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 processes. Refer to Section 4.1 System Engineering Technical Reviews (SETRs) / Integrated Master Plan (IMP) for more information.

Finally, SEs and SSEs will update the Functional Thread Analysis and the architecture to the lowest level through the SSE 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 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 2.2-1.

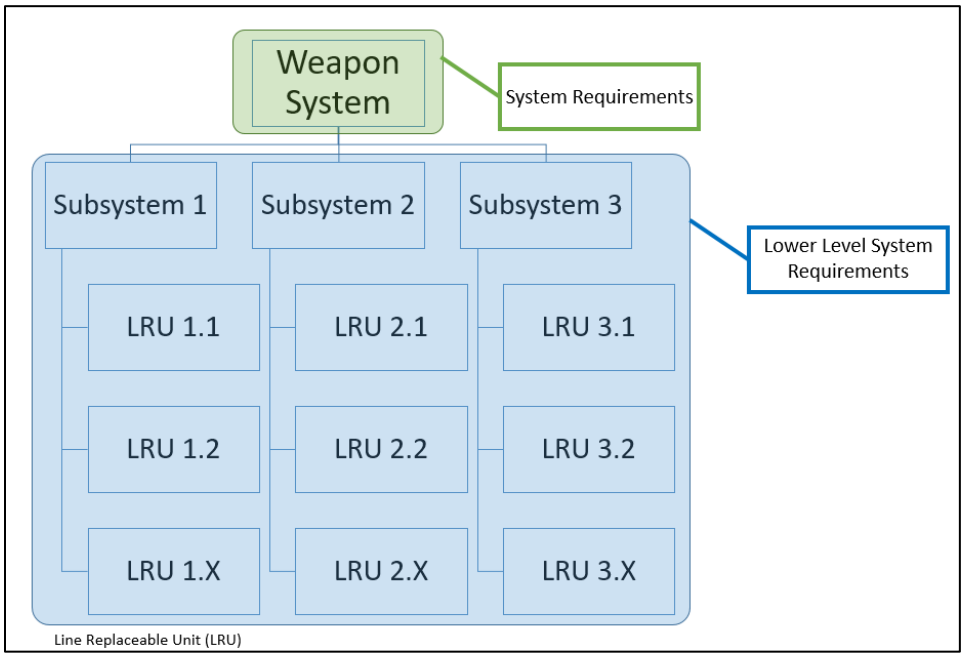


FIGURE 2.2-1: Example Specification Tree.

Table 2.2-1 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 reference Attachment 1 for more detail on the requirements in this table.

TABLE 2.2-1: 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 encrypt transmissions and communications for data 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 encrypt data 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 are hardened 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/sub-systems, 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
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	The system shall continually monitor input/output parameters.

Figure 2.2-2 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 2.2-2 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 800-53r4 where applicable.

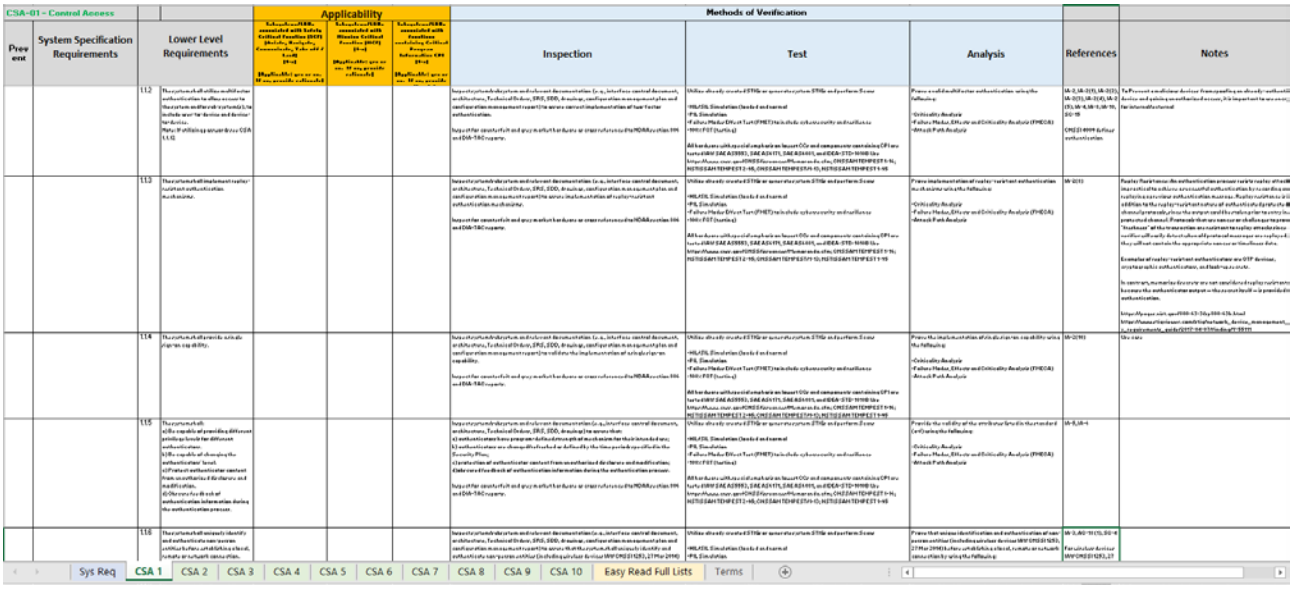


FIGURE 2.2-2: Attachment 1 Example - SRD/System Specification derivation from the Prevent, Mitigate, and/or Recover and to the CSAs.

2.3 Statement of Objectives (SOO) and Statement of Work (SOW).

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 800-53R4 controls (refer to Attachment 3).

2.3.1 Program Protection.

A. The contractor shall deliver a Program Protection Implementation Plan (PPIP). The contractor shall integrate the PPIP activities in the Integrated Master Plan/Integrated Master Schedule (IMP/IMS). The contractor shall derive requirements from the PPIP and put into specification(s), trace, and verify through the Systems Engineering Processes. Program Protection includes the following areas: Cybersecurity to include Trusted Systems and Networks (TSN), Cyber Resiliency, Anti-Tamper, and Information Protection. The contractor shall utilize modeling and simulations for verification of specifications. The contractor shall accredit and verify modeling and simulation used for closure of any specification requirements in accordance with MIL-STD-3022. All paragraphs below shall be contained in the PPIP. The Government shall be able to participate in all testing. In addition, the contractor shall allow the Government time in the laboratories and with the weapon system to conduct Penetration testing. The contractor shall conduct its own weapon system penetration testing and provide the test plan, procedures and reports (CDRLs 1, 2, 3, 4, 5, 6, 7, 8, 9, 34, 35, 36, and 37 per Attachment 2.)

B. The contractor shall utilize Digital Engineering for the derivation of requirements from the PPIP, trace, and verify through the Systems Engineering Processes for execution of Program Protection requirements verification through Systems Engineering Practices (CDRL 8 per Attachment 2.)

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

C. The contractor shall perform a Program Protection / System Security Risk Assessment of the system per section 1.10, Risk Management of the USAF System Security Engineering Acquisition Guidebook, utilizing the System Security Working Groups. These risks shall be part of the program risks. Contractor shall also provide a System Safety Plan and perform a System Safety Hazard Analysis. The contractor shall provide a cyber requirements implementation assessment per Appendix F of the USAF Weapon System Program Protection/Systems Security Engineering Guidebook. In addition, the contractor shall provide courses of action with cost details to get all risk to below medium (CDRLs 10, 11, 46 and 47 per Attachment 2.)

D. The contractor shall establish and maintain an incident response infrastructure with identified membership and operating procedures to facilitate rapid response to cybersecurity incidents as documented in the Security Plan/Security Assessment 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), and to the Defense Cyber Crime Center (DC3) via the DIBNet and Joint Deficiency Reporting System. In addition, provide a root-cause, corrective-action report. (CDRL 12 and 16 per Attachment 2.)

NOTE: DIBNet is a web portal for sharing threat information between DoD and Defense Industrial Base (DIB) companies.

E. 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 13 and 14 per Attachment 2.)

F. The contractor shall perform 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 weapon system that are potential avenues for covert storage and/or timing channels (CDRL 38 per Attachment 2.)

2.3.2 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) at: https://www.acq.osd.mil/se/initiatives/init_pp-sse.html, and the DoD CIO website at: http://dodcio.defense.gov/Library/.

A. The contractor shall provide a Security Plan for the system. The contractor shall provide a Security Assessment Plan, a Security Assessment Report, and a Plan of Action and Milestones (POA&M). The contractor shall ensure the weapons system's configuration has been baselined and documented to meet the cyber requirements (CDRLs 3, 4, 5, 16, 17, 23, 42, 43, and 44 per Attachment 2.)

NOTE: The Chief Information Security Officer and the Authorizing Official (AO) shall approve the Cybersecurity Strategy and Security Plan prior to RFP and/or proposal release and continue to assess and update through the lifecycle. There are additional areas the Program Office will be required to address in the Security Plan/Security Assessment Plan (SP/SAP). The Security Plan in CDRL 16 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 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. In addition, the contractor shall ensure the Failure Modes Effects Analysis (FMEA) trace to the Criticality Analysis, which are documented in the Failure Modes Effects Criticality Analysis (FMECA). 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 (CDRLs 18, 19 and 20 per Attachment 2.)

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.

C. 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 20 per Attachment 2.)

D. The contractor shall allocate system security and 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 800-53R4 (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 Resiliency requirements. The contractor shall allocate requirements to the Safety Critical Functions (SCFs), Mission Critical Functions (MCFs), and 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 matrix. The contractor shall ensure integration and verification that SCFs, MCFs, and CPI have the appropriate segregation and diverse redundancy in the architecture to complete the mission (resiliency), see requirement section for more information. In addition, the Architect Design Document shall include an 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 segregation and diverse redundancy is maintained for the SCF, MCF, and functions associated with CPI (CDRLs 7 and 21 per Attachment 2.)

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, IAW the current version of CNSSD No. 505 and NIST SP 800-161, 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). The contractor shall develop and implement a Counterfeit Parts Prevention Program 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 (CDRLs 16, 22, 23, 31, 39, 40, and 41 per Attachment 2.)

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) 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. 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 (CDRLs 3 (STP), 5 (STR), 23, 24, 25, 26, 32, 43, 44, and 45 per Attachment 2.)

G. The contractor shall develop an NSA-approved Key and Certificate Management Plan (KCMP) for each cryptographic system. 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 Section 2.3.2.A (CDRL 27 per Attachment 2.)

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 28 per Attachment 2.)

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 at: https://apps.nsa.gov/iaarchive/programs/iad-initiatives/tempest.cfm

I. The contractor shall provide the information required for the program office to obtain Interim Authority To Test (IATT) and Authority To Operate (ATO) (CDRL 29 per Attachment 2.)

2.3.3 Critical Program Information (CPI) / Anti-Tamper (AT).

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 AT Desk Reference and Anti-Tamper Technical Implementation Guide (TIG), 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 30 per Attachment 2.)

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

2.3.4 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.

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 33 per Attachment 2.)

C. The contractor shall provide Operations Security (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.

D. **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 at: https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html

1) *The Contractor shall, upon request, 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 Special Publication (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 transmitted. The Contractor shall, upon request, provide the government with access to the system security plan(s) (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. (CDRL 15 per Attachment 2.)*

2) 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 15 per Attachment 2.)

a) 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.

3) 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 15 per Attachment 2.)

E. 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 15 per Attachment 2.)

F. 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 15 per Attachment 2.)

G. 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) unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer (DoD CIO) (CDRL 23 per Attachment 2.)

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 SETRs (see Section 4 of this guidebook).

3.0 Solicitation Documents.

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

3.1 Request for Proposal (RFP) – Contract Clauses and Provisions.

An RFP is a solicitation used in negotiated 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. http://acqnotes.com/acqnote/tasks/request-for-proposalproposal-development

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 DoD 5220.22-M 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.

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

1. ***52.204-2 Security Requirements (AUG 1996).***
   - URL: https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#i1063713 https://www.acquisition.gov/?q=/browse/far/52
   - 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).***
   - URL: https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#id1669B0A0E67
   - 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).

- URL: https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#i1064072
- 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).

- URL: https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#i1049272
- 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 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 (DFARS) Clauses and Provisions.

The following DFARS clauses and provisions are recommended in AF contracts, when applicable:

1. 252.204-7000 Disclosure of Information (Oct 2016).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7000
- 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.

2. 252.204-7003 Control of Government Personnel Work Product (Apr 1992).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7003
- 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.

3. 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls (OCT 2016).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7008
- 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 NISTSP 800-171.

4. 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (OCT 2016).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7009
- 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.

5. 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
- 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.

6. 252.208-74 Enterprise Software Agreements (Revised 30 OCT 2015).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/208_74.htm#208.7402
- 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. http://www.esi.mil

7. 252.209.7002 Disclosure of Ownership or Control by A Foreign Government (JUN 2010).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252209.htm#252.209-7002
- Source*:* PART 209 – Contractor Qualifications, SUBPART 209.1 – Responsible Prospective Contractors.
- Rationale for Use*:* 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.

8. 252.211-7003 Item Unique Identification and Valuation (MAR 2016).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252211.htm#252.211-7003
  Source*:* PART 211 – Describing Agency Needs, SUBPART 211.2 – Using and Maintaining Requirements Documents.
- Rationale for Use*:* 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.

9. 252.225-7048 Export-Controlled Items (JUN 2013).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252225.htm#252.225-7048
- Source: PART 225 — Foreign Acquisition**,** SUBPART 225.79 — Export Control.
- Rationale for Use: 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.

10. 252.225-7049 Prohibition on Acquisition of Commercial Satellite Services from Certain Foreign Entities—Representations (Jan 2018).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252225.htm#252.225-7049
- Source: PART 225 – Foreign Acquisition**,** SUBPART 225.772-5 – Solicitation provision.
- Rationale for Use: 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 (AT&L) or Under Secretary of Defense for Policy [USD (P)].

11. 252.239-7000 Protection Against Compromising Emanations (OCT 2019).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7000
- Source: PART 239 – Acquisition of Information Technology, SUBPART 239.71 – Security and Privacy for Computer Systems.
- Rationale for Use: 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.

12. 252.239-7001 Information Assurance Contractor Training and Certification (JAN 2008).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7001
- 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.

13. 252.239-7009 Representation of Use of Cloud Computing (SEP 2015).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7009
- 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.

14. 252.239-7010 Cloud Computing Services (OCT 2016).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7010
- 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/.

15. 252.239-7017 Notice of Supply Chain Risk (FEB 2019).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7017
- 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. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

16. 252.239-7018 Supply Chain Risk (FEB 2019).

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7018
- 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.

17. 252.246-7003 Notification of Potential Safety Issues (JUN 2013).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7003
- 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.

18. 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System (AUG 2016).

- URL: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007
- 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.

19. Software Assurance DFARS Clauses and Provisions

- URL: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252227.htm
- Rationale for Use: The following 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.
- 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
  https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_538779.pdf

  - ***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)**

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

The following AFFARS clauses and provisions are recommended in all AF contracts, where applicable:

1. **5352.204-9000 Notification of Government Security Activity and Visitor Group Security Agreements *(Oct 2017).***
   - URL: http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/af_afmc/affars/5352.htm#P29_2417
   - 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 DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).

2. ***5352.215-9000 Facility Clearance (MAY 1996).***
   - URL: http://farsite.hill.af.mil/archive/AFFARS/2006-1003/5352.htm#P80_5027
   - 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).***
   - URL: http://farsite.hill.af.mil/reghtml/Regs/far2afmcfars/AF_AFMC/Affars/5352.htm#p53522429000
   - 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).***
   - URL: http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/af_afmc/affars/5352.htm#P285_22522
   - 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 (RFP) – 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 (https://cs2.eis.af.mil/sites/23230/RFPResource/SitePages/Home.aspx) 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 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) 800-53R4 controls per DoDI 8500.01 and DoDI 8510.01).*
2. *Cyber Resiliency techniques and approaches as required by the SOO/SOW, SRD/Spec, SP/SAP, and Architecture.*
3. *A description of the Anti-Tamper (AT) Plan in accordance with DoDI 5200.39 and 5200.47.*
4. *Information Protection as required by the DD Form 254 and Security Classification Guide.*
5. *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.*
6. *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.*

3.3 Request for Proposal (RFP) – 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 offerors 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 (RFP) – Cost Volume - SSE Cost Estimate.

The RFP – Cost Volume 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. 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: https://at.dod.mil.

4.0 Government Acquisition Activities.

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

4.1 Systems Engineering Technical Reviews (SETRs) / Integrated Master Plan (IMP).

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 tech reviews (9 primary tech 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 A:

Section 2.3.1 Program Protection.

Section 2.3.2 Cybersecurity, Cyber Resiliency, and Trusted Systems and Networks.

Section 2.3.3 Critical Program Information (CPI) / Anti-Tamper (AT).

Section 2.3.4 Security Management / Information Protection.

These SETR entrance and exit criteria should be included in the IMP in the contract. Having the SETR entrance and exit criteria in the IMP and on contract is critical to program success.

4.1.1 Alternative Systems Review (ASR) or EMD Contract Award.

ENTRY CRITERIA for Program Protection	SOO/SOW
PPP, developed IAW DoD Outline & Guidance, approved by Milestone Decision Authority (MDA) IAW DoDI 5000.02, Table 2.	Section 2.3.1
SSE risks, developed IAW the AF SSE Guidebook, reviewed in conjunction with programmatic risks.	Section 2.3.1.B
All SSE requirements (Cybersecurity, TSN, CPI/AT, SCRM, V&V Testing, DD Form 254, DFARS) are all adequately articulated in the EMD RFP (contract clauses, SRD, SOO/SOW).	N/A Govt Task
SSE is reflected in program planning documents [e.g., SEP, TEMP, RMP, Lifecycle Sustainment Plan (LCSP)].	N/A Govt Task

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency , and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.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.B
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic Bearing Components (LBC) submitted to DIA TAC.	Section 2.3.2.C
System architecture, developed utilizing CA, MCFs, SCFs, and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP), and included as in the CS/CSP/SP.	Section 2.3.2.D
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 2.3.2.E
Software Assurance (SwA) - SwA requirements for software CCs from the CA are documented in the PPP and reflected in the EMD SOW.	Section 2.3.2.F

ENTRY CRITERIA for Critical Program Information (CPI) / Anti-Tamper (AT)	SOO/SOW
AT Plan, developed IAW ATEA guidance, approved by ATEA and Program Executive Officer (PEO).	Section 2.3.3.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 Govt Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.2 Systems Requirements Review (SRR).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, System Spec, RMP, Digital Engineering models/tools/source data, and cyber incidents).	Section 2.3.1.A,B,C,D
SSE Requirements Implementation Assessment CDRL reviewed and the SSE Requirements Implementation Assessment developed per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, reviewed and any changes approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic Bearing Components (LBC) updated and submitted to DIA TAC.	Section 2.3.2.C
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D
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 2.3.2.E
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP and PPP. The SwA requirements are based on the FTA.	Section 2.3.2.F

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
AT Plan, developed IAW ATEA guidance, reviewed and, any changes have been approved by ATEA and Program Executive Officer (PEO).	Section 2.3.3.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 Govt Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.3 System Functional Review (SFR).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, System Spec, Allocated specs (HW& SW), RMP, Digital Engineering models/tools/source data, and cyber incidents).	Section 2.3.1.A,B,C,D
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from SRR updated to include the lower-level requirements assessment per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency , and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, reviewed and any changes approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic Bearing Components (LBC) updated and submitted to DIA TAC.	Section 2.3.2.C
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D
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 2.3.2.E
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP and PPP. The SwA requirements are based on the FTA.	Section 2.3.2.F

ENTRY CRITERIA for Critical Program Information (CPI) / Anti-Tamper (AT)	SOO/SOW
AT Plan, developed IAW ATEA guidance, reviewed and any changes have been approved by ATEA and Program Executive Officer (PEO).	Section 2.3.3.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 Govt Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.4 Preliminary Design Review (PDR)

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, System Spec, Allocated specs (HW& SW), Subsystems Spec and CI specs, RMP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from SFR updated to include the component level assessment per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency , and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, reviewed, and any changes approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic Bearing Components (LBC) updated and submitted to DIA TAC.	Section 2.3.2.C
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D
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 2.3.2.E
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP and PPP. The SwA requirements are based on the FTA.	Section 2.3.2.F
An initial attack path analysis is completed and approved.	Section 2.3.1 F
Modeling and simulation accreditation and verification & validation plan completed and approved.	Section 2.3.1 A
Configuration Management Plan completed and approved.	Section 2.3.2 A
Initial Configuration Management Report completed and approved.	Section 2.3.2 A

ENTRY CRITERIA for Critical Program Information (CPI) / Anti-Tamper (AT)	SOO/SOW
AT Plan, developed IAW ATEA guidance, reviewed and any changes have been approved by ATEA and Program Executive Officer (PEO).	Section 2.3.3.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 Govt Task

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.5 Critical Design Review (CDR).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A, Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, System Spec, Allocated specs (HW & SW), Subsystems Spec and CI specs, RMP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Traceability Matrix).	Section 2.3.1.A, 2.3.2.D
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from PDR updated per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, reviewed and any changes approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
Hardware Assurance (HwA) – Critical Components (CC) from the CA containing Logic Bearing Components (LBC) updated and submitted to DIA TAC.	Section 2.3.2.C
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D
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 2.3.2.E

Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP and PPP. The SwA requirements are based on the FTA.	Section 2.3.2.F
TEMPEST control plan reviewed.	Section 2.3.2.H
Modeling and simulation accreditation and verification & validation report completed and approved.	Section 2.3.1 A
An attack path analysis is completed and approved.	Section 2.3.1 F
Final Configuration Management Report completed and approved.	Section 2.3.2 A

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	**SOO/SOW**
Draft Anti-Tamper Evaluation Plan (ATEP), developed IAW ATEA guidance, reviewed.	Section 2.3.3.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 Govt Task

ENTRY CRITERIA for Security Management / Information Protection	**SOO/SOW**
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.6 Test Readiness Review (TRR).

ENTRY CRITERIA for Program Protection	**SOO/SOW**
SSE risks developed IAW the AF SSE Guidebook, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Traceability Matrix).	Section 2.3.1.A
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from CDR updated per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, and Trusted Systems and Networks	**SOO/SOW**
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
TEMPEST control plan reviewed.	Section 2.3.2.H
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D

ENTRY CRITERIA for Critical Program Information (CPI)/Anti-Tamper (AT)	SOO/SOW
Anti-Tamper Evaluation Plan (ATEP), developed IAW ATEA guidance, approved by ATEA and Program Executive Officer (PEO).	Section 2.3.3.A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.7 Functional Configuration Audit (FCA).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, Traceability Matrix).	Section 2.3.1.A
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from TRR updated per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency , and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, reviewed, and any changes approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP and PPP. The SwA requirements are based on the FTA.	Section 2.3.2.F
TEMPEST control plan reviewed.	Section 2.3.2.H
A subsystem attack path analysis is finalized and approved.	Section 2.3.1 F
Updated and finalized Configuration Management Report completed and approved.	Section 2.3.2 A
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D

ENTRY CRITERIA for Critical Program Information (CPI) / Anti-Tamper (AT)	SOO/SOW
Anti-Tamper Evaluation Report (ATER), developed IAW ATEA guidance, reviewed.	Section 2.3.3.A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.8 System Verification Review (SVR).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g. PPIP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Test CDRL submittals reviewed (e.g., test plans and procedures, test reports, and Traceability Matrix).	Section 2.3.1.A
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from FCA updated per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency , and Trusted Systems and Networks	SOO/SOW
Security Plan (SP), developed IAW DoD guidance and/or NIST SP 800-18, reviewed, and any changes approved by the Authorizing Official (AO).	Section 2.3.2.A
Security Assessment Plan (SAP), developed IAW NIST SP 800-53A, reviewed.	Section 2.3.2.A
Security Assessment Report (SAR), developed IAW NIST SP 800-53A, App G, reviewed.	Section 2.3.2.A
PPP Criticality Analysis (CA) appendix updated with information from the Functional Thread Analysis (FTA) report, reviewed and approved.	Section 2.3.2.B
Software Assurance (SwA) - The plan for implementing the SwA requirements is documented in the SDP and PPP. The SwA requirements are based on the FTA.	Section 2.3.2.F
TEMPEST control plan reviewed.	Section 2.3.2.H
An attack path analysis is finalized and approved.	Section 2.3.1 F
Updated and finalized Configuration Management Report completed and approved.	Section 2.3.2 A
System architecture, developed utilizing the FTA and mitigations to SSE risks, agreed to by the AO, TSN, ATEA, and Information Protection (IP) and included as in the CS/CSP/SP.	Section 2.3.2.D

ENTRY CRITERIA for Critical Program Information (CPI) / Anti-Tamper (AT)	SOO/SOW
Anti-Tamper Evaluation Report (ATER), developed IAW ATEA guidance, reviewed.	Section 2.3.3.A

ENTRY CRITERIA for Security Management / Information Protection	SOO/SOW
Security Classification Guide (SCG), developed IAW DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.9 Production Readiness Review (PRR).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task
SSE CDRL submittals reviewed (e.g., PPIP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Requirements Implementation Assessment CDRL reviewed and the assessment from SVR updated per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency, and Trusted Systems and 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.B

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 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

4.1.10 Physical Configuration Audit (PCA).

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 2.3.1
SSE risks developed IAW the AF SSE Guidebook, updated, and reviewed in conjunction with programmatic risks.	Section 2.3.1.B
SSE is reflected in program planning documents (e.g., SEP, TEMP, RMP, LCSP).	N/A Govt Task

SSE CDRL submittals reviewed (e.g., PPIP, Digital engineering Models/tools/source data, and Cyber incidents).	Section 2.3.1.A,B,C,D
SSE Requirements Implementation Assessment CDRL reviewed and the assessment PRR updated per Appendix F.	Section 2.3.1.C

ENTRY CRITERIA for Cybersecurity, Cyber Resiliency , and Trusted Systems and 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.B

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 DODM 5200.45, reviewed by EZIP and approved by the PEO within the last 5 years.	N/A Govt Task

Attachment 1 – Cybersecurity and Resiliency System and Lower Level Specification Requirements.

Embedded in this attachment is the "Cybersecurity and Resiliency System and Lower Level Specification Requirements" excel workbook. This workbook contains a worksheet for system-level requirements as well as multiple worksheets for the lower-level system requirements (see Figure A1-1). The Excel workbook is intended to be used by the engineering workforce experienced in DoD acquisitions.

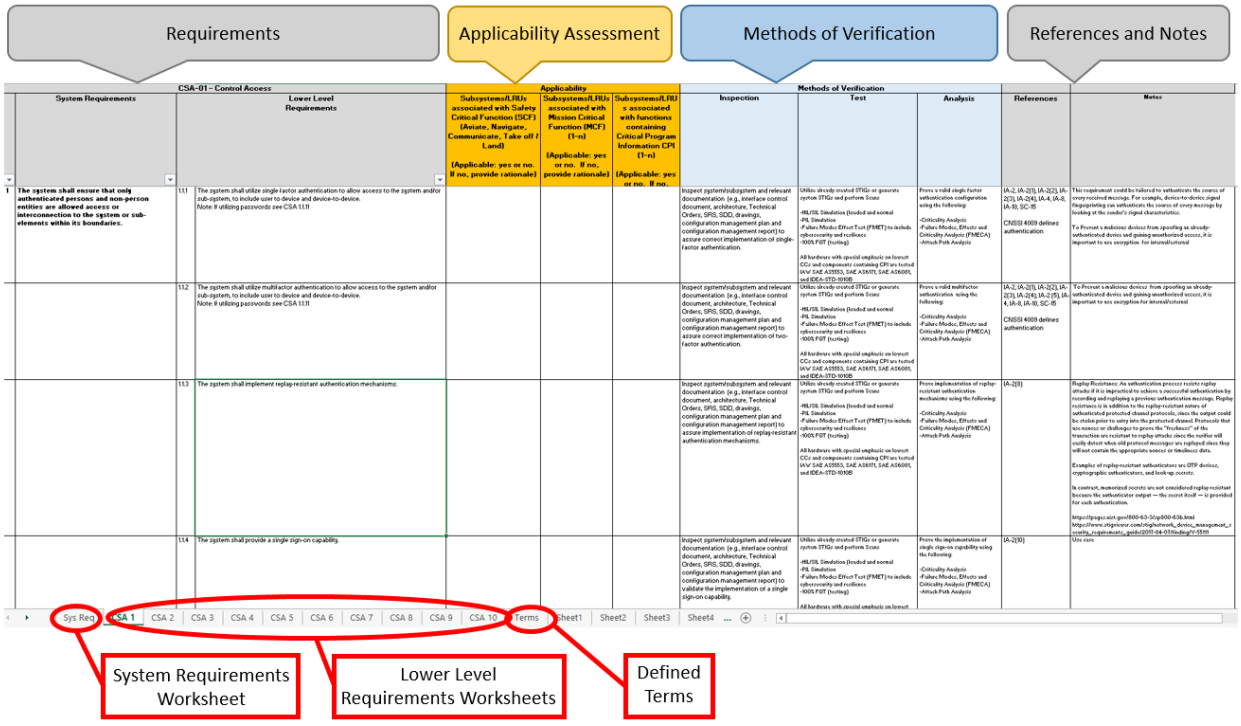


FIGURE A1-1: Example SRD/System Specification Excel.

As stated in Section 2.2 System Requirements Document (SRD) and System Specifications, identify which system level requirements are applicable to the system based off the Functional Thread Analysis. Once the system level requirements are identified/selected as applicable, then the lower-level system requirements shall be selected using the CSA worksheets (**NOTE:** applicability of the lower-level system requirements shall be determined based of the Functional Thread Analysis, just as the system-level requirements were).
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 (CDRLs) Associated with SSE.

This table lists all the CDRLs referenced in the Statement of Objectives/Statement of Work (SOO/SOW) sample contract language in Section 2.3 of this appendix. Each SOO/SOW example in Section 2.3 lists the corresponding CDRLs using the numbering system in the table below.

All the CDRLs in this table will not apply to every program. The program should first determine the SOO/SOW paragraphs for SSE that apply to their program. Those paragraphs will list recommended CDRL numbers, which can be found in the table below. The recommended CDRLs should then be individually reviewed for applicability to each program office, and they can also be tailored as needed.

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 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 • 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 • Update annually	Follow the newest OSD PPP template
2.3.1 A	2	Specification	Program-Unique Specification Documents	DI-SDMP-81493, or DI-IPSC-81431A	Standard program delivery	
			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 A 2.3.2 A 2.3.2 F (STP only)	3	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	

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)**
			Test and Evaluation Program Plan (TEPP)	DI-NDTI-81284	• 150 days prior to test • 60 days prior to Test Readiness Review	
			Software Test Plan (STP)	DI-IPSC-81438	• Draft 30 days prior to PDR • Final 60 days prior to Test Readiness Review	
2.3.1 A 2.3.2 A	4	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 A 2.3.2 A 2.3.2 F (STR only)	5	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)].*
			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	
2.3.1 A	6	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	
2.3.1 A	7	Traceability Matrix	Technical Report Study/Services (addressing Traceability Matrix)	DI-MISC-80508	90 days prior to PDR, CDR, TRR, FCA, SVR	
2.3.1 A 2.3.1 B	8	Models, Tools and Source data for the Digital Engineering	Technical Report Study/Services (addressing Models, Tools and Source data for the 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.
2.3.1 A	9	Interface Control Documents (ICDs)	Interface Control Document (ICD)	DI-SESS-81248	150 days prior to CDR, FCA, SVR	

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 C	10	Risk Management	Contractor's Risk Management Plan	DI-MGMT-81808	Standard program delivery	
			Technical Report Study/Services (addressing Risk Assessment Report)	DI-MISC-80508	Standard program delivery	
2.3.1 C	11	COAs with Cost Technical Report	Technical Report Study/Services (addressing the Cost Technical Report)	DI-MISC-80508	Standard program delivery	
2.3.1 D	12	Cyber Incidents	Technical Report Study/Services (addressing the Incident, Root Cause, and Corrective Action)	DI-MISC-80508	• Draft report 24 hours after incident • Final report 10 days after incident	
2.3.1 E	13	Meeting Minutes and Action Items	Conference Minutes	DI-ADMN-81250	30/60 days after meeting	
2.3.1 E	14	Agenda	Conference Agenda	DI-ADMN-81249	30 days prior to meeting	
2.3.2 A 2.3.4 D 2.3.4 E 2.3.4 F	15	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	
2.3.1 D 2.3.2 A 2.3.2 E	16	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	

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	17	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, 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, architecture 120 days prior to Authority To Authorize (ATO) • Update as required	
2.3.2 B	18	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	
2.3.2 B	19	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 B 2.3.2 C	20	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	
2.3.2 D	21	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)	
2.3.2 E	22	Manufacturing Plan	Customized Microelectronics Devices Source Protection Plan	DI-MGMT-81763	Standard program delivery	
			Counterfeit Prevention Plan	DI-MISC-81832	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)**
			Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report	DI-QCIC-80125	Standard program delivery	
			Technical Report Study/Services (addressing the Manufacturing Program Plan)	DI-MISC-80508	Standard program delivery	
2.3.2 A 2.3.2 E 2.3.2 F 2.3.4 G	23	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	
2.3.2 F	24	Software Development Plan	Software Development Plan (SDP)	DI-IPSC-81427B	• Preliminary draft 30 days prior to System Requirements Review (SRR) • Draft due 45 days after System Functional Review (SFR) • Final due 30 days after Government approval • After Government approval, contractor shall submit subsequent revisions to address contractor proposed changes	
2.3.2 F	25	Software Requirement 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	
			Software Product Specification (SPS)	DI-IPSC-81441	• Due 30 days prior to FCA for each associated CSCI • Final due 30 days prior to PCA for each associated CSCI	
2.3.2 F	26	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	
			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	

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)**
			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	
			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	
2.3.2 G	27	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	
2.3.2 H	28	TEMPEST Control Plan	TEMPEST Control Plan	DI-MGMT-81026	• 150 days prior to test • Final 30 days after test completion	
			TEMPEST Test Plan	DI-EMCS-81683	• 150 days prior to test • Final 30 days after test completion	
			TEMPEST Test Evaluation Report	DI-EMCS-81684	• 150 days prior to test • Final 30 days after test completion	
2.3.2 I	29	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)**
2.3.3 A	30	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 Verification and Validation (V&V) Plan 60 days prior to PDR • Final V&V 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.
			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	
2.3.2 E	31	Information Systems Security (INFOSEC) Anonymity Plan (IAP)	Information Systems Security (INFOSEC) Anonymity Plan (IAP)	DI-MGMT-81717	Standard program delivery	
2.3.2 F	32	Information Security (INFOSEC) Boundary Configuration Management Plan	Information Security (INFOSEC) Boundary Configuration Management Plan	DI-SESS-81343	Standard program delivery	
2.3.4 B	33	Operations Security (OPSEC) Plan	Operations Security (OPSEC) Plan	DI-MGMT-80934	Standard program delivery	
2.3.1 A	34	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	

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 A	35	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 A	36	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 A	37	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	
2.3.1 F	38	Attack Path Analysis Report	Technical Report Study/Services (addressing Attack Path Analysis)	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	
2.3.2 E	39	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	
2.3.2 E	40	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	
2.3.2 E	41	Acceptance Test Report	Acceptance Test Report (ATR)	DI-QCIC-81891	• 30 days after test completion	

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	42	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	
2.3.2 A	43	Configuration Management Plan	Technical Report Study/Services (addressing overall System Configuration)	DI-CMAN-80858B	• 60 days prior to PDR • Update as required	
2.3.2 A	44	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	
2.3.2 F	45	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 C	46	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	
2.3.1 C	47	Hazard Assessment	System Safety Plan	DI-SAFT-81626	Standard program delivery	
			System Safety Hazard Analysis Report	DI-SAFT-80101	Standard program delivery	

Attachment 3 – SOO/SOW Requirements Trace.

2.3.1: Program Protection	NIST SP 800-53r4 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	AC, AU, CA, CM, CP, IA, PL, SA, SC, SI	CSA 01, CSA 05, CSA 06, CSA 07, CSA 08, CSA 09, CSA 10
C	CA, PM, SA	CSA 06, CSA 08
D	AC, AU, CP, IR, PE, SE, SI	CSA 05, CSA 07, CSA 08, CSA 09
E	AC, CM, SA	CSA 01, CSA-06, CSA-10
F	AC, CA, RA, SA, SC, SI	CSA 01 through CSA 10
2.3.2: Cybersecurity and Trusted Systems and Networks	**NIST SP 800-53r4 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]
I	AU, CA, PL, PS, RA, SA	CSA-01, CSA 04, CSA 06, CSA 07, CSA 10
2.3.3: Critical Program Information (CPI) / Anti-Tamper (AT)	**NIST SP 800-53r4 Control Family References**	**CSEIG "Highly Applicable" Mapping**
A	AC, PE, SA	CSA 01, CSA 08
2.3.4: Security Management / Information Protection	**NIST SP 800-53r4 Control Family References**	**CSEIG "Highly Applicable" Mapping**
A	AC, PE, PS	CSA-01
B	CA, CP, SA, SC	CSA 01, CSA 02, CSA 03, CSA 05, CSA 06, CSA 08
C	AT, CP, IR, PL, PM, SA	CSA 05, CSA 10
D	AC, SI	CSA 01, CSA 06, CSA 10
E	AC, AU, CP, IR, MA, PE, PL, PM, SA, SC, SI	CSA 01, CSA 05, CSA 06, CSA 07, CSA 08, CSA 09, CSA 10
F	AC, AU, CP, IA, MP, PE, SA, SC,	CSA 01, CSA 03, CSA 05, CSA 07, CSA 08
G	AC, AU, CA, CM, IA, IR, MA, PE, PL, PS, SA, SC, SI	CSA 01, CSA 03, CSA 06, CSA 07, CSA 08, CSA 09, CSA 10

Attachment 4 – Weapon System Cybersecurity Guidance – Operational Cyber Hygiene

To address these Weapons System Cybersecurity risks, the Cyber Resiliency Office for Weapon Systems, in collaboration with Air Force Task Force Cyber Secure, identified five cyber hygiene best practices (ref. Table A4-1). These cyber hygiene practices are traceable to the SRD/System Specifications based on the CSA decomposition and mapped into Table A4-1.

For more information on the Feb 02 2017 Operational Cyber Hygiene Memo, dated Feb 02, 2017, visit the USAF Acquisition System Security Primer site https://www.milsuite.mil/wiki/USAF_Acquisition_System_Security_Primer.

TABLE A4-1: CSAs Mapped to Cyber Hygiene.

"Criteria" System Specification Requirements Mapping	Cyber Hygiene Practices	Current Operations	Future Operations
CSA 07 (7.1), CSA 08 (8.1), CSA 10 (10.1)	**Anti-Virus Scanning**	Conduct routine anti-virus scans on traditional IT systems (i.e., Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
CSA 01 (1.1), (1.2), CSA 02 (all), CSA 03 (3.1) CSA 04 (4.1), (4.2), CSA 07 (7.1), (7.3)	**External media**	Place configuration control processes on all external media (i.e., USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e., USB whitelisting). Implement processes to monitor logs and audit usages.
CSA 04 (all)	**Data Integrity**	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data (i.e., digital signatures).
CSA 01 (1.2)	**Administrative Privileged Accounts**	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
CSA 01-08 (all)	**Purposed Equipment**	Ensure mission support systems (i.e., mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e., application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e., Windows XP).

APPENDIX B – USAF Process Guide for Critical Program Information (CPI) and Critical Component (CC) Identification

VERSION 2.0

12 March 2020

FOREWORD

Comments, suggestions, or questions on this document should be captured in the Comment Resolution Matrix (CRM) in Appendix K, and e-mailed to the Cyber Resiliency Office for Weapon Systems (CROWS@us.af.mil).

RECORD OF CHANGES.

Version	Date	Summary
v2.0	Mar 2020	Updated with changes from comments from the National Defense Industrial Association (NDIA) Systems Security Engineering Committee. Changed terminology from "validate" CPI to "approve" throughout, improved content describing the CPI Identification Analysis step, added references to useful tools, added Horizontal Protection Guide and Low Observable/Counter Low Observable references throughout, updated template table for Candidate CPI List, and replaced "criticality level" with "Consequence of Compromise" throughout.
v1.1	May 2018	Using the merged document, identified several duplicative steps between the two processes. Developed a more fully integrated/single CPI and CC Identification Process. Generated content to conduct the integrated CPI and CC Identification process while also allowing for a single process to be conducted. Added content to reflect the possibility that the program may not have a CPI determination. Changed “criticality value” to “criticality level” to reflect AFPAM 63-113. Added content to reflect DoDI 5200.44, Change 2, and its emphasis on industrial control systems and spare and replacement parts. Incorporated a few additional changes of an editorial nature. Eliminated separate process diagram figures with red blocks around specific process steps. Removed the three-part NAR briefing templates from the appendices; they are available separately. STAR was replaced with VOLT. Content regarding the NAR process was streamlined. Updated references to latest versions/dates. Beefed up the CPI and CC Identification Analysis sections with additional content. Updated CPI content to align with direction from Anti-Tamper Executive Agency (ATEA) Program Office. Moved first two steps of CC identification to Prerequisites, Establish Technical/Engineering Foundation as it pertains to both CPI and CC. ASDB, now back online, is reflected in the document. Corrected content to reflect that the MDA validates CPI and CC determinations.

		Incorporated comments received from CRMs.
v1.0a	July 2016	USAF Process Guide for Critical Program Information (CPI) and Critical Component (CC) Identification – initial team development effort that merged the Engineering Instruction for CPI Identification and the Engineering Instruction for CC Identification into a single document. This collaborative effort included the Air Force Life Cycle Management Center, the Air Force Space and Missile Systems Center, and the Air Force Nuclear Weapons Center.

TABLE OF CONTENTS

List of Figures

List of Tables

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.

United States Air Force (USAF) 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.

1 Introduction.

During program protection planning, a set of activities is performed to manage the execution of program protection. The Critical Program Information (CPI) Identification Process and the Critical Component (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. United States Air Force (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 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[1] 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 validated by the Milestone Decision Authority (MDA)[2]. The validated 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/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.

[1] 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 TABLE 6-4

[2] 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.

3 Integrated CPI and CC Identification Process Flow.

The integrated CPI and CC Identification Process Flow (see FIGURE 3-1) 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.

  Note: The list of tables in the "Program Protection Plan (PPP)" box on FIGURE 3-1 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 and agencies/organizations involved in a program, additional coordination steps with pertinent organizations may be necessary.

Significant information associated with a specific program/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.

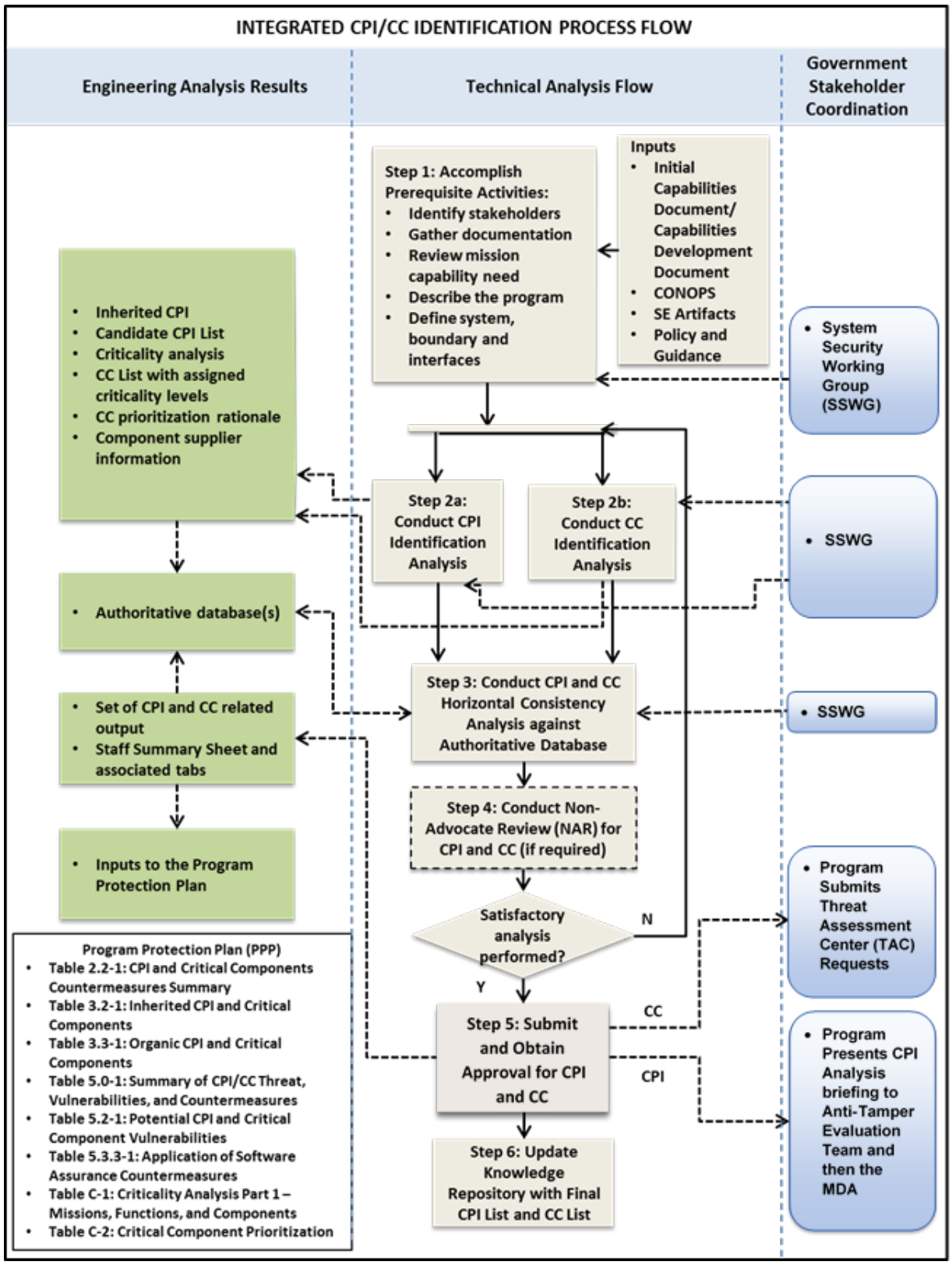


FIGURE 3-1. Integrated CPI and CC Identification Process Flow.

4 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 0) 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 4-1. This figure can be used to maintain focus on the CPI Identification Process being executed by your program. Each rectangle in the figure corresponds with the associated step number (i.e., steps 2a, 3, 4, 5, and 6) in Figure 3-1 above and discussed later in this guide. The relevant content in the associated sections provide the guidance needed to execute each step.

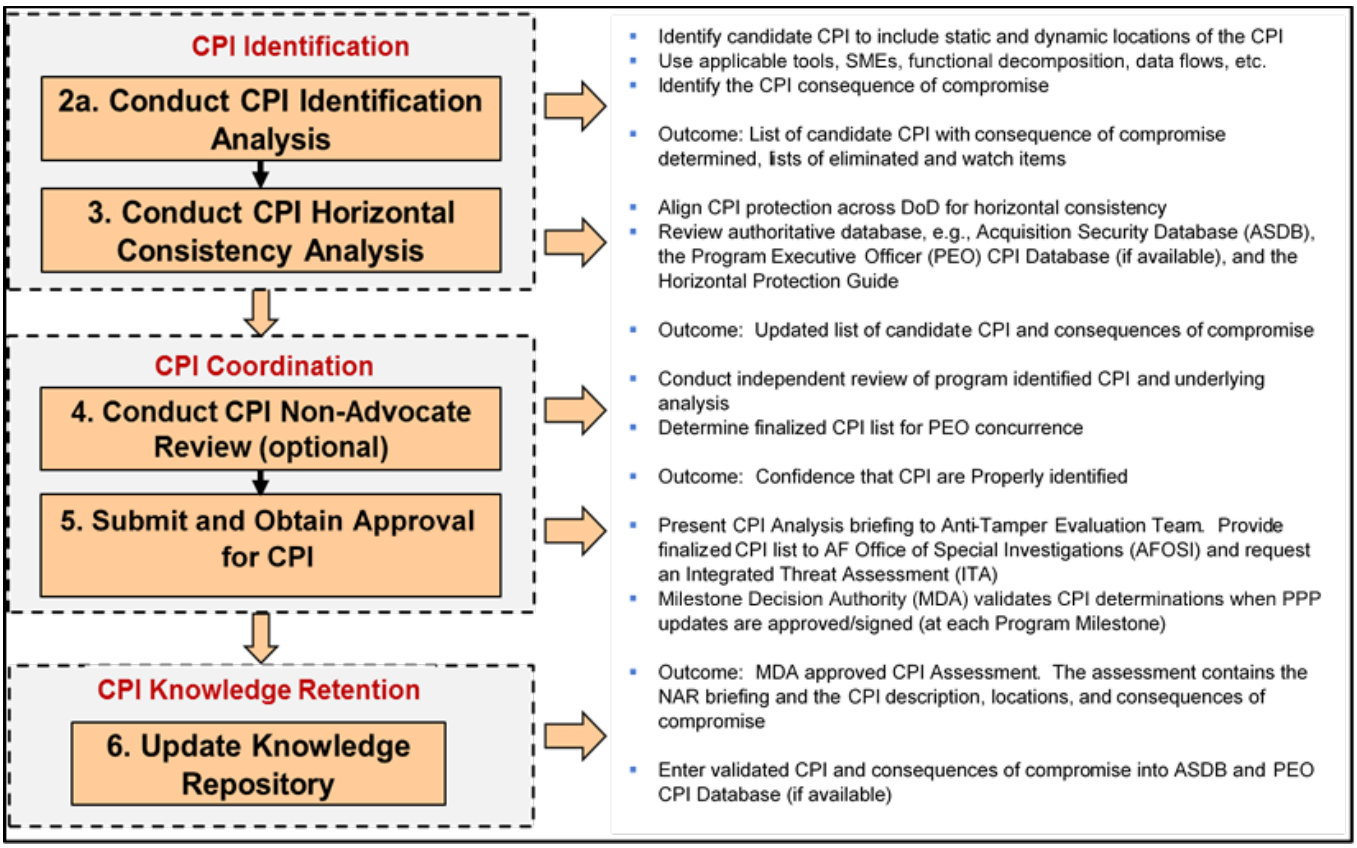


FIGURE 4-1. CPI Identification Process.

4.2 Individual CC Identification Process.

For programs executing only the CC Identification Process, refer to FIGURE 4-2. This figure can be used to maintain focus on the CC Identification Process being executed by your program. Each rectangle in the 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.

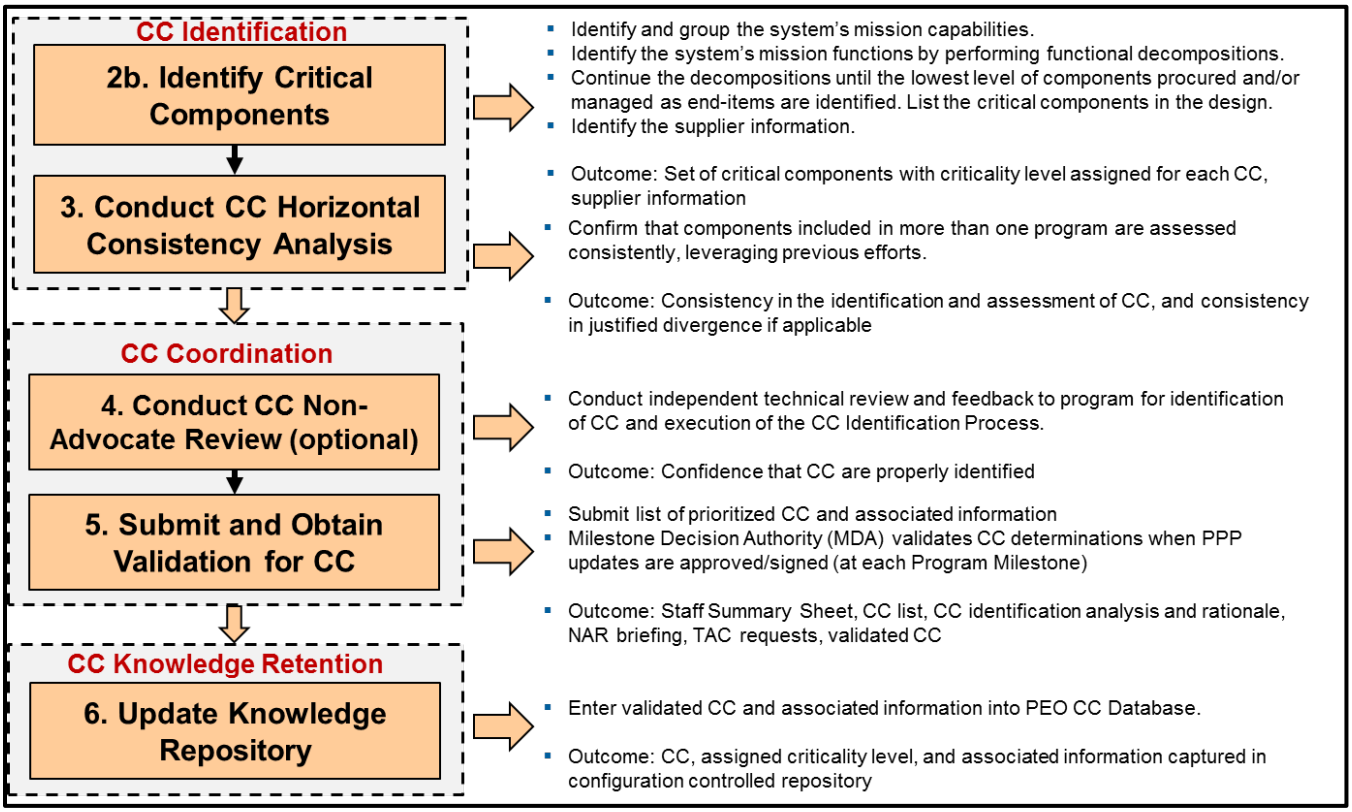


FIGURE 4-2. CC Identification Process.

5 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
- 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 5-1 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 5-1. 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]) • Capability Development Document (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 • Initial Capabilities Document (ICD) • System Performance Specification
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		• 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 (ICD) • 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) • Horizontal Protection Guide (HPG) • Information Support Plan (ISP) • 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) • Test and Evaluation Master Plan (TEMP) • Tri-Service Committee (TSC) or EXCOM Decision Memorandums (DMs) from the program • Use Cases • Validated On-line Life-cycle Threat (VOLT) Report

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 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, 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 which 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 Systems[6]

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.

Potential Inputs:

- CONOPS.
- ICD/CDD.

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

- ISP.
- KPPs.
- Use Cases.
- 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 the Boundary and Interfaces for the System-of-Interest and the Enabling Systems.

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 Step 2: Conduct CPI and CC Identification Analyses.

6.1 Step 2a: Conduct CPI Identification Analysis.

Step 2a, Conduct CPI Identification Analysis (see FIGURE 3-1), 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 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 ATEA, 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 Horizontal Protection Guide, DoDM S-5230.28, 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 (DoDM S-5230.28, expert opinion, 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 DoDM S-5230.28" (required for export license applications), whether the CPI meets or breaks DoDM S-5230.28 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 Guidebook (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; Horizontal Protection Guide; 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

which 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 which 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. The questions contained in all service tools, including AFPAM 63-113, are based on questions that pre-dated the 2015 version of DoDI 5200.39. Many of these questions are irrelevant at best, or misleading.

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 11.1 for a list of CPI resources and Section 11.2 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):

- 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).
https://www.dodtechipedia.smil.mil/ASDB

- Horizontal Protection Guide – available from the DoD Anti-Tamper Executive Agent (ATEA) Program Office. The guide is classified Secret and should be used in conjunction with other resources in the development of candidate CPI.

- 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.
http://static.e-publishing.af.mil/production/1/saf_aq/publication/afpam63-113/afpam63-113.pdf

- USD (I) CPI Identification Survey Tool (AFPAM 63-113, Attachment 8) – provides several questions to assist programs with their critical thinking.
http://static.e-publishing.af.mil/production/1/saf_aq/publication/afpam63-113/afpam63-113.pdf

- 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 2: 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 3: DCS cases should contact the ATEA on the proper 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 [7] 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).
- ICD/CDD.
- 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.

[7] 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)."

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

- 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.
- ICD/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.

Guidance:

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.

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.
- ICD/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 B-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.
- ICD/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.
- ICD/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.

Specific task outcomes and supporting information can be organized and captured in template form, similar to that suggested by the template in

TABLE 6-1.

TABLE 6-1. 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 6-1 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 Residency – (Resident or Non-Resident)
- 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 Resident CPI (No R-CPI).
- Determination of inherited Resident CPI (R-CPI) that does not require additional protection.

Guidance:

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. For example, if it resides on the weapon system, maintenance system, training systems/devices, or any part of the exposed or delivered system, the CPI would be considered Resident-CPI.
- 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 not resident on the delivered system still requires its protection needs to be addressed; however, this CPI might not be subject to AT protections.

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 inTABLE 6-2 can be used.

TABLE 6-2. 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.

Summary: 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 6-3 may be used to organize and capture possible CPI items that may emerge in the future.

TABLE 6-3. CPI Watch List (Template).

Name of Possible CPI	CPI Description

Potential Inputs:

- Results of technical analyses
- List of CPI items eliminated as candidates

Outcome:

- List of possible CPI items to watch for future review and analysis

Guidance:

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 (see FIGURE 3-1), 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 6-4. Definitions for System Terms.

System	Combination of interacting elements organized to achieve one or more stated purposes.
System Element	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 other 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

Adapted from ISO/IEC/IEEE 15288:2015 "Systems and Software Engineering - System Life Cycle Processes"

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 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.
- ICD/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.

Summary: 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.

Potential Inputs:

- CONOPS.
- ICD/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).

Outcome:

- 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 3: Map the Mission Critical Functions to the System Architecture and 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.

The scope of this task is limited to Information and Communications Technology (ICT) components (refer to **Error! Reference source not found.** for definition). It is important to ensure that all CCs designed into the system-of-interest and in 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:
        1. Provide a path of unmediated (direct or immediate) access to a CC.
        2. Are able to interfere with the behavior of a CC.
        3. Provide separation of security domains.
        4. 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, 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.

Guidance:

- 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.

7 Step 3: Conduct CPI and CC Horizontal Consistency Analyses.

7.1 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. It also facilitates use of and maintains the DoD CPI Horizontal Protection Guide. 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

The 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 7-1 illustrates how CPI is identified, protected, and verified across the DoD services.

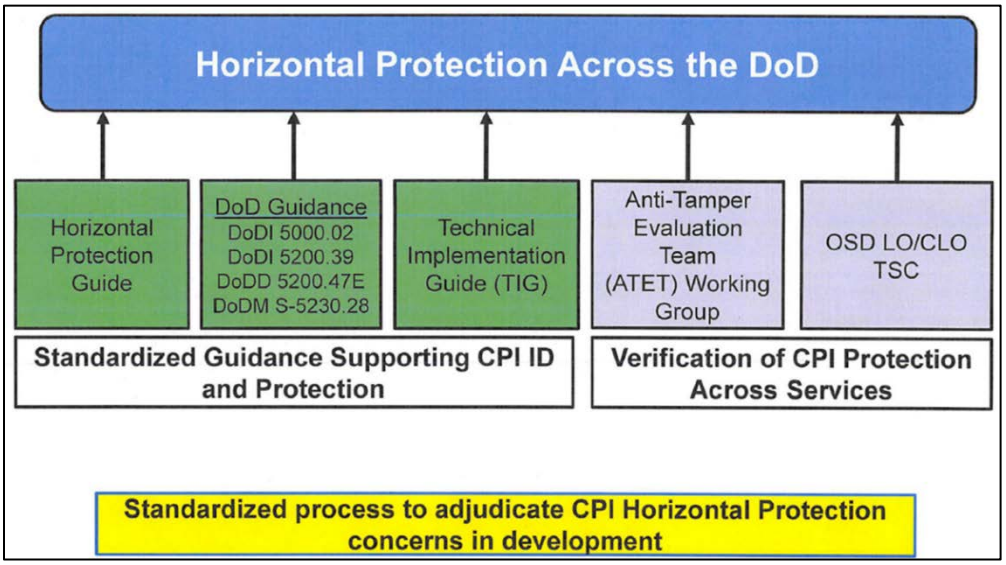


FIGURE 7-1: Horizontal Protection

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.
- ICD, 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.

7.1.1 Conduct CC Horizontal Consistency Analysis.

Conduct CC Horizontal Consistency Analysis (see FIGURE 3-1) increases the consistency 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.

- Task 2.3: For components that do not have the same criticality level, determine if the difference is justified. 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.

8 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 Level (CofC) 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 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.

NAR Objective:

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 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** – Once the program is ready to proceed with a NAR, 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.

9 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."

9.1 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 R-CPI determination, a No R-CPI Memorandum [12] should be completed and submitted with the program's signed PEO Staffing Package, which constitutes the "R-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 (including the No R-CPI Memorandum) 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 R-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.

9.2 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.

9.3 Update PPP Document and Obtain Approval of CPI and 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 3-1). The MDA approves the CPI and CC determinations when the PPP is approved.

10 Step 6: 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.

11 References.

The following documents are referenced in this guide:

1. DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), 28 May 2015, Incorporating Change 2, October 15,2018
2. DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), Incorporating Change 2, July 27, 2017
3. DoDI 5000.02, Operation of the Defense Acquisition System, Change 5, October 21, 2019
4. ISO/IEC/IEEE 15288:2015, “Systems and Software Engineering – Systems Lifecycle Processes”
5. Deputy Assistant Secretary of Defense - Systems Engineering, Program Protection Plan Outline & Guidance, Version 1.0, July 2011
6. (U) DoD Anti-Tamper (AT) Technical Implementation Guidebook (TIG) (Document is classified SECRET), 30 November 2016
7. AFPAM 63-113, Program Protection Planning for Life Cycle Management, 17 October 2013
8. Department of Defense Anti-Tamper Desk Reference, Second Edition, April 2017
9. DoDM S-5230.28, (U) Low Observable (LO) and Counter Low Observable (CLO) Programs Manual (Document is classified SECRET), 28 December 2016
10. Memorandum for ESC/CPSG, Subject: Policy for ESC/CPSG Programs and Air Force Anti-Tamper (AT) Office, SAF/AQLS, involvement, May 28, 2008
11. Defense Acquisition Guidebook (https://www.dau.mil/tools/dag)
12. Memorandum for SAF/AQLS, Subject: Anti-Tamper (AT) Plan Requirement for Program XYZ

11.1 CPI Informational Resources.

The following informational resources should be reviewed prior to beginning the CPI Identification analysis (links provided where available):

- Industrial Base Technology List – describes science and technology capabilities, by category, under global development. The list provides high level descriptions to supplement more technical guidance provided by other resources. https://www.cdse.edu/documents/cdse/CI-JobAidSeries-IBTL.pdf

- In 2009, the Administration launched the Export Control Reform Initiative (ECR Initiative) which will fundamentally reform the U.S. export control system. The technology categories are being revised and published for public comment. For additional information, refer to: http://2016.export.gov/ecr/index.asp

  The U.S. Department of Commerce's International Trade Administration provides practical advice and business tools at: https://www.export.gov/welcome

- International Traffic in Arms Regulation (ITAR)

  https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987

11.2 Other References.

Other relevant sources associated with program protection planning, CPI, and CC include the following documents:

- Department of Defense Directive (DoDD) 5200.47E, Anti-Tamper (AT), Change 2, 31 August 2018
- DoDI 4140.67, DoD Counterfeit Prevention Policy, Change 2, August 31, 2018
- Air Force Policy Directive 63-1/20-1, Integrated Life Cycle Management, 3 June 2016
- Air Force Instruction 63-101/20-101, Integrated Lifecycle Management, 9 May 2017
- "CPI Assessment and Identification Guide (CAIG) v. 1.0," NDIA, 2 Aug 2019 (FOUO) https://at.dod.mil/
- "CPI/LO/CLO Workbook Template 1.0", NDIA, 2 Aug 2019 (FOUO) https://at.dod.mil/
- "CPI/LO/CLO Workbook Template 1.0 - Classified HPG and 5230 Tabs," 2 Aug 2019 (SECRET), document request through of https://at.dod.mil/
- Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, April 6, 2015

APPENDIX C – Functional Thread Analysis & Attack Path Analysis

1. Background.

The Functional Thread Analysis (FTA) begins by completing a functional decomposition. The functional decomposition starts with the system mission capabilities identified in the user requirement documents (i.e. Initial Capabilities Document (ICD), Capabilities Design Document (CDD)). Capabilities from the user documents are already prioritized based on the associated Key Performance Parameters (KPPs). The capabilities are then further decomposed and allocated to the mission(s) required for the system to deliver the capabilities. Missions need to be prioritized by the High Performance Team (HPT) (Appendix A: USAF SSE Acquisition Guidebook, section 1.1.2). Missions can further be decomposed to the functions required to execute the mission. While conducting the functional decomposition, it is necessary to identify functions that are mission critical as well as safety critical. Mission Critical Functions (MCFs) are defined per DoDI 5200.44 as, “any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed.” Safety Critical Functions (SCFs) are defined per MIL-STD-882 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 how to implement cybersecurity and cyber resiliency requirements. Functions can then be further allocated to the systems/subsystems/Line-Replaceable Units (LRUs)/components required to execute these functions. A program may contain Critical Program Information (CPI), which can be associated with particular functions. CPI is defined per DoDI 5200.39 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.

A graphical representation of this decomposition is in Figure C-1.

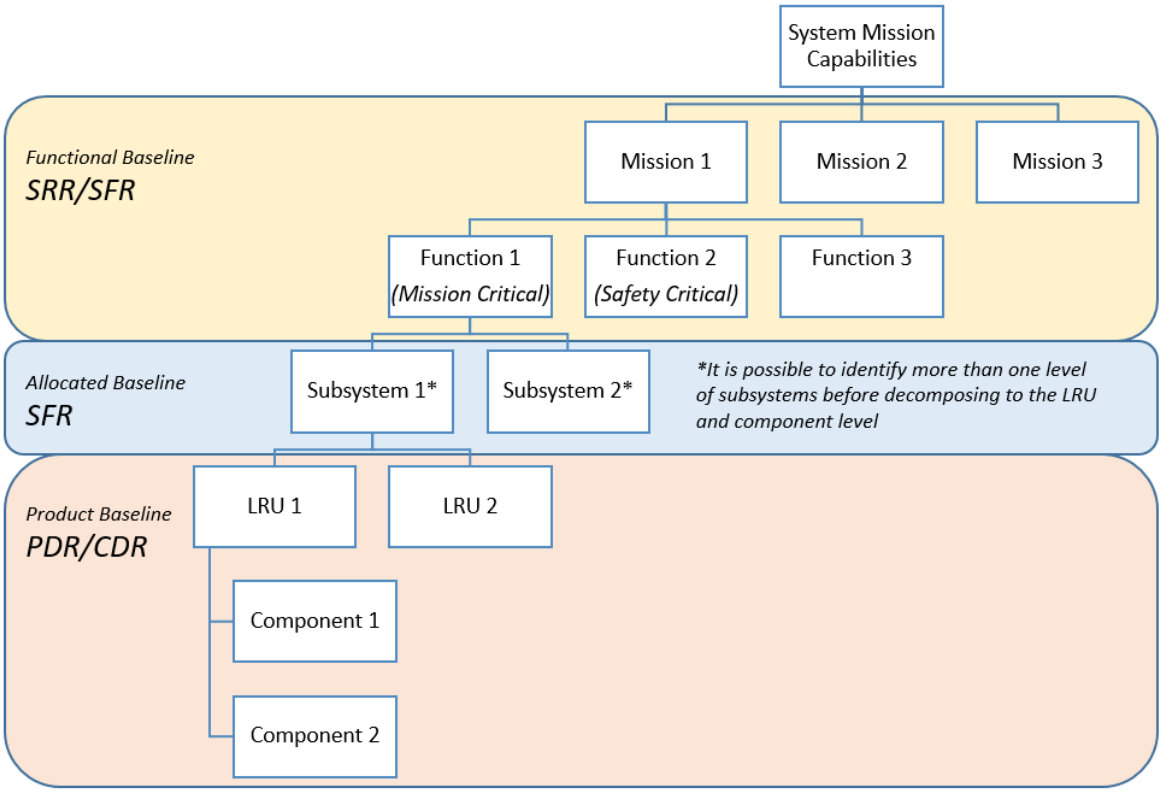


FIGURE C-1: Functional Decomposition Example.

2. Scope.

The scope of this appendix is to provide guidance on how to functionally decompose a system to the component level, and understand the potential vulnerabilities within the system through the analysis of attack paths.

It is important to note that the FTA is an iterative process that should be updated in conjunction with a program's Systems Engineering Technical Reviews (SETRs). The fidelity of the analysis will increase as the program matures through its lifecycle. The earliest steps of the FTA occur within the activities to characterize the system in WBS 1.2 (see Figure C-2). Further details regarding the expectation of fidelity are located in the subsequent sections. Since cyber is a continually evolving and growing threat to all weapon systems, it is critical to factor in active threat data and operational experience that may impact future design changes, upgrades, mitigations and/or the development of new Tactics, Techniques, and Procedures. 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). The tables in the FTA process are populated from this information/data.

Figure C-2 illustrates the FTA, Attack Path Analysis (discussed in Section 5 of this appendix), corresponding outputs (i.e., reports), and the follow on cyber test activities. Figure C-2 also maps the activities for the FTA and Attack Path Analysis back to the corresponding Work Breakdown Structure (WBS) for the USAF Weapon System PP and SSE Process step. Ultimately, conducting the FTA and Attack Path Analysis during the execution of the USAF Weapon System PP and SSE Process, programs will establish informed risks. The risk assessment(s) should

then be used to assist the program in determining where and how mitigations can be applied to ensure the weapon system design addresses operations in cyber-contested environments. Mitigating these risks should be done through allocation/implementation of the SSE requirements located in Appendix A: USAF SSE Acquisition Guidebook, Attachment 1 Excel workbook.

APPENDIX C

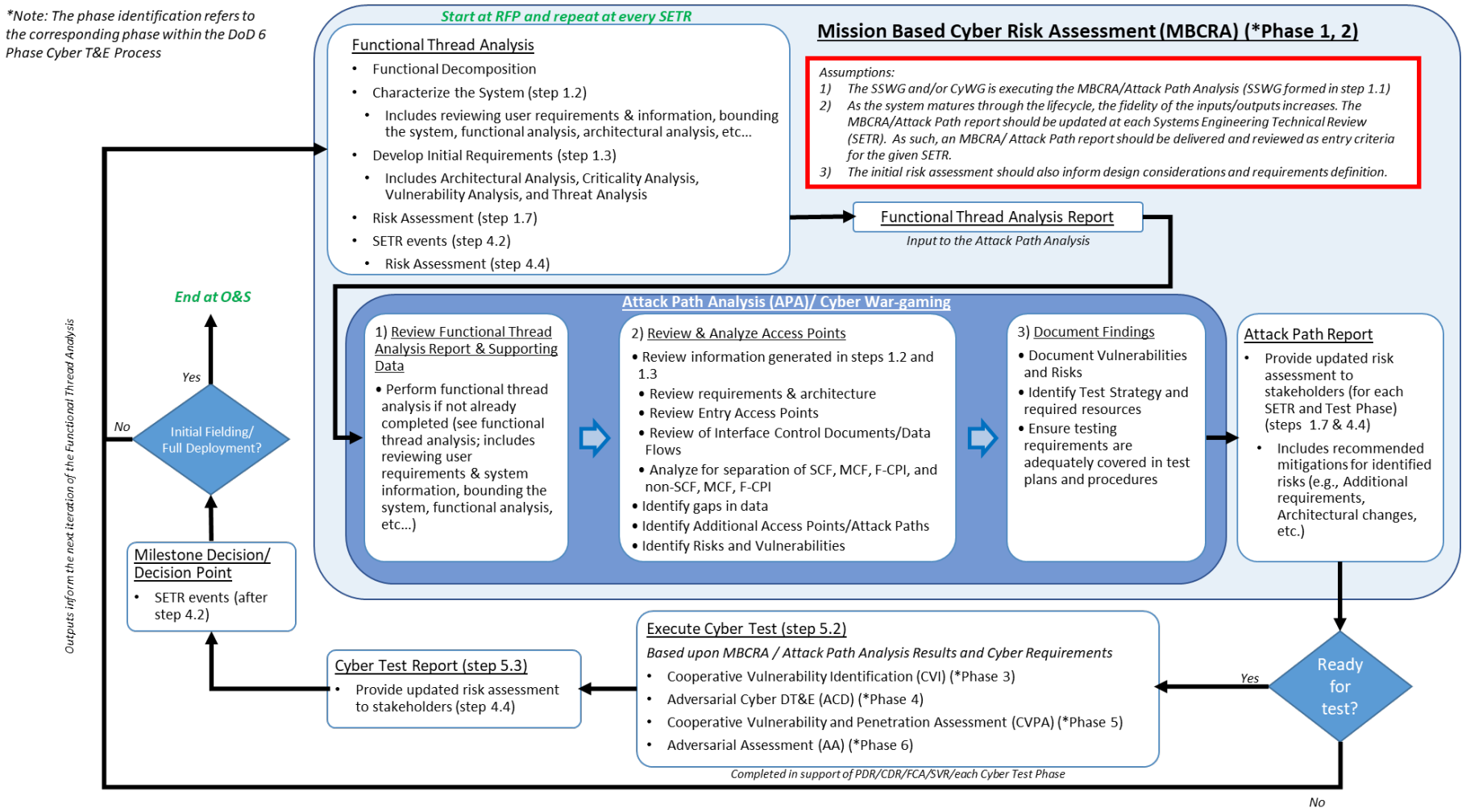


FIGURE C-2: FTA and Attack Path Analysis Summary.

3. FTA Supporting System Requirements Review (SRR).

3.1 Documents to Review.

- User Requirements (ICD, CDD), to include the applicability of the Cyber Survivability Attributes (CSAs) as seen in Table C-1 example below. If the information in Table C-1 is not provided in the ICD or CDD, then the Program Office will need to develop.
- System Requirements Document (SRD) or System Specification, to include the applicable system level requirements from Appendix A: USAF SSE Acquisition Guidebook, Attachment 1 Excel file
- 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.*

TABLE C-1: Example CSA Applicability to MCFs, SCFs, and Functions associated with CPI.

	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 in accordance with DoDI 5200.44 and CNSSI No. 1253 (i.e. impact levels for confidentiality, integrity, or availability), 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).

3.2 Information to Document in the FTA Report.

- Operational objectives/tasks
- MCFs, SCFs, and Functions associated with CPI
- The mission including the MCFs, SCFs, and Functions associated with CPI (see table C-2)
- System attributes such as boundaries, adjacency/dependency; internal/external to system connections; type/functionality; redundancy, etc. (see Table C-3)
- All known data sources and data receivers.

- Updated Risk Assessment per Work Breakdown Structure (WBS) for the USAF Weapon System Program Protection (PP) and Systems Security Engineering (SSE) Process, step 4.4 Risk Assessment.

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 size 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 in accordance with DoDI 5200.44 and CNSSI No. 1253 (i.e. impact levels for confidentiality, integrity, or availability), 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-3: MCFs/SCFs/CPI Functions to 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) that details the interfaces, where possible.

4. FTA supporting System Functional Review (SFR).

The FTA from SRR will be updated to reflect the additional information in support of SFR. Additionally the information developed during the FTA will support the attack path analysis and the risk assessment for PDR and CDR.

5. Documents to review.

- SRR FTA
- User Requirements (ICD, CDD)
- System Requirements Document (SRD)
- System and subsystem specifications, to include 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 applicable*

5.1 Information to Document in the FTA Report.

- MCFs, SCFs, and Functions associated with CPI mapped to the subsystems that are responsible for those functions (see Table C-4)
- The manufacturer (mfg) responsible for each subsystem (see 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. (see Table C-5)
    - *Include known service type, linkages and type, directionality, digital/analog, etc.*
- All known data sources and data receivers.
- Updated Risk Assessment per Work Breakdown Structure (WBS) for the USAF Weapon System PP and SSE Process, step 4.4 Risk Assessment.

APPENDIX C

TABLE C-4: Systems and Subsystems Responsible for MCFs, SCFs, and functions associated with CPI.

	Mission 1 *(mfg)*			**Mission 2** *(mfg)*		**Mission 3** *(mfg)*	**Criticality / Consequence**
	Subsystem a *(mfg)*	Subsystem b *(mfg)*	Subsystem c *(mfg)*	Subsystem b *(mfg)*	Subsystem d *(mfg)*	Subsystem e *(mfg)*	
MCF 1							
MCF 2							
SCF 1							
SCF 2							
CPI 1							
CPI 2							

The size 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 in accordance with DoDI 5200.44 and CNSSI No. 1253 (i.e. impact levels for confidentiality, integrity, or availability), 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) that details the subsystem to subsystem interfaces.

6. FTA supporting Preliminary Design Review (PDR) and Critical Design Review (CDR)

The FTA from SFR is updated to include the detailed system design information at PDR. Subsequently, the PDR FTA is updated for CDR. Documents reviewed and information required in the PDR and CDR FTA reports should be considered initial and final (respectively). The information developed during the FTA will support the attack path analysis and risk assessment(s).

6.1 Documents to review.

- SFR FTA
- User Requirements (ICD, CDD)
- 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
- Information Support Plan
- 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 applicable.*

6.2 Information to Document in the FTA Report.

- Complete identification of LRUs and components responsible for the MCFs, SCFs, and functions, and functions associated with CPI (see Tables C-6 and C-8)
- The manufacturer (mfg) responsible for each LRU and component (see Tables C-6 and C-8). *NOTE: Once manufacturers are known, DIA TACs should be submitted.*
- LRUs mapped to the LRUs (see Table C-7) and components mapped to the components (see Table C-9)
    - All boundaries, interfaces identified, entry access points, function, ports and protocols, configuration management, etc.
- All known data sources and data receivers.
- Updated Risk Assessment per Work Breakdown Structure for the USAF Weapon System PP and SSE Process, step 4.4 Risk Assessment.

APPENDIX C

TABLE C-6: Systems, Subsystems, and LRUs Responsible for MCFs, SCFs, and functions associated with CPI

	Mission 1							Mission 2				Mission 3		Criticality / Consequence
	Subsystem a *(mfg)*			Subsystem b *(mfg)*		Subsystem c *(mfg)*		Subsystem b *(mfg)*		Subsystem d *(mfg)*		Subsystem e *(mfg)*		
	LRU 1 *(mfg)*	LRU 2 *(mfg)*	LRU 3 *(mfg)*	LRU 2 *(mfg)*	LRU 4 *(mfg)*	LRU 3 *(mfg)*	LRU 5 *(mfg)*	LRU 2 *(mfg)*	LRU 4 *(mfg)*	LRU 6 *(mfg)*	LRU 7 *(mfg)*	LRU 4 *(mfg)*	LRU 7 *(mfg)*	
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 (i.e. impact levels for confidentiality, integrity, or availability), 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-7: LRUs to LRUs Interfaces (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 Interface Control Document identifier(s) that details the LRU to LRU interfaces.

APPENDIX C

TABLE C-8: Systems, Subsystems, LRUs, and Components Responsible for MCFs, SCFs, and functions associated with CPI .

	Mission 1															**Mission 2**										**Mission 3**					**Criticality / Consequence**
	Subsystem a *(mfg)*							Subsystem b *(mfg)*					Subsystem c *(mfg)*			Subsystem b *(mfg)*					Subsystem d *(mfg)*					Subsystem e *(mfg)*					
	LRU 1 *(mfg)*			LRU 2 *(mfg)*		LRU 3 *(mfg)*		LRU 2 *(mfg)*		LRU 4 *(mfg)*			LRU 3 *(mfg)*		LRU 5 *(mfg)*	LRU 2 *(mfg)*		LRU 4 *(mfg)*			LRU 6 *(mfg)*			LRU 7 *(mfg)*		LRU 4 *(mfg)*			LRU 7 *(mfg)*		
Component (mfg)*	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 size 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 (i.e. impact levels for confidentiality, integrity, or availability), 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).

APPENDIX C

TABLE C-9: Components to Components Interfaces (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 Interface Control Document identifier(s) that details the component to component interfaces.

7. Attack Path Analysis.

The Attack Path Analysis focuses on where the threat (i.e. attacker) can gain access to the system/subsystem (i.e., entry access points), and which paths can be used to attack/exploit the system (targets are primarily MCFs, SCFs, and functions associated with CPI). It builds upon/uses the information documented in the FTA. The attack path analysis should be completed in support of PDR and then updated at CDR (refer to the Work Breakdown Structure (WBS) for the USAF Weapon System PP and SSE Process, step 4.2.5 Preliminary Design Review and step 4.2.7 Critical Design Review). The Attack Path Analysis should be updated following any design changes that may impact potential attack paths through the systems. Additionally, the Attack Path Analysis should be updated after conducting cyber test that invalidates previous attack path theories or discovers previously undocumented paths into or through the system.

Attack paths should be assessed based on risk. This includes analyzing the likelihood of occurrence based on threat actor known or projected capabilities to execute an attack (i.e. is the attack technically feasible). It also includes analyzing the consequence of an attack. Detailed information on how to conduct a risk assessment is located in Appendix A: USAF SSE Acquisition Guidebook, section 1.10. If a risk is considered unacceptable, further actions are required by the program to mitigate the risk.

7.1 Documents to review.

- Completed PDR FTA and CDR FTA
- SRD
- Specifications (System, subsystem, LRU, component, HW, SW, etc…)
- Interface Control Documents and Data Flows
- Completed system level and subsystem level architectures to include the following DoD Architecture Framework viewpoints:
    - *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 applicable.
- Architecture functional models
- Failure Modes Effects and Criticality Analysis (FMECA) (reference CDRL 19 in Appendix A: USAF SSE Acquisition Guidebook, Attachment 2)
- Fault Tree Analysis

7.2 Questions to Consider.

When asking the questions below, it is important to analyze both the intelligence (i.e., Blue Team) and counter intelligence (i.e., Red Team) viewpoints.

- 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 entry access point(s) (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 potential mission effects could be realized if an adversary is able to exploit the identified 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?

An Entry Access Point (EAP) allows an adversary entrance into the system. It is a virtual or physical system component that allows entry to a system/sub-system or provides a path through the system/sub-system/LRU/component. EAPs establish the edge of the cyber-attack surface or a system's cyber boundary and are a starting point for an attack path into the system.

7.3 Example Methodologies

- Cyber Test Prioritization Methodology (CTPM) Guide
- Assessing Cyber Threats and Risks to DoD Weapon Systems - Attack Path Analysis Model
- Wheel of Access
- Cyber Table Top
- Cyber War Gaming

7.4 Information to Document in the Attack Path Analysis Report

- Boundaries and interfaces evaluated
- Subsystems/LRU/component Access Points and the trace of connections to the access points/entry points
- Results of the analysis (i.e., identified vulnerabilities)
    - Updated Risk Assessment per Work Breakdown Structure for the USAF Weapon System PP and SSE Process, step 4.4 Risk Assessment.
- Cyber failure modes
- Recommended mitigations for vulnerabilities

8. FTA beyond CDR.

The FTA is an ongoing assessment post CDR through operational deployment, where the operational assessments/re-assessments will occur. This includes ensuring sustainment, monitoring of maintenance, supply chain, upgrades, etc. are fully addressed and implemented. Update FTA based on threat, configuration management, use data, etc. Additionally the information developed during the FTA will support the risk assessments for the life of the program.

APPENDIX D – Example Use Cases

The following use cases are examples of how to apply the processes within this guidebook, using fictitious weapon systems, and walking step by step through the WBS activities. Uses cases with examples from multiple domains will be added in future versions of this guidebook to demonstrate how the process (tailoring the SSE requirements, in particular) can vary depending on the type of USAF weapon system being developed.

Current use cases:

Chapter 1: Aircraft System

Future additions planned:

Chapter 2: Space System

Chapter 3: Nuclear Weapon System

Chapter 4: Command and Control (C2) System

Chapter 5: Non-Nuclear Weapon

Chapter 1: Aircraft System Use Case

The following Aircraft System Use Case utilizes the Systems Engineering process framework to incorporate program protection elements into a weapon system. This Use Case is divided into two segments: first, incorporation of program protection into a new start program; and two, the tailored steps for a modification, or upgrade, to an existing fielded weapon system. **Figure D-1** identifies the overall process flow used for these activities.

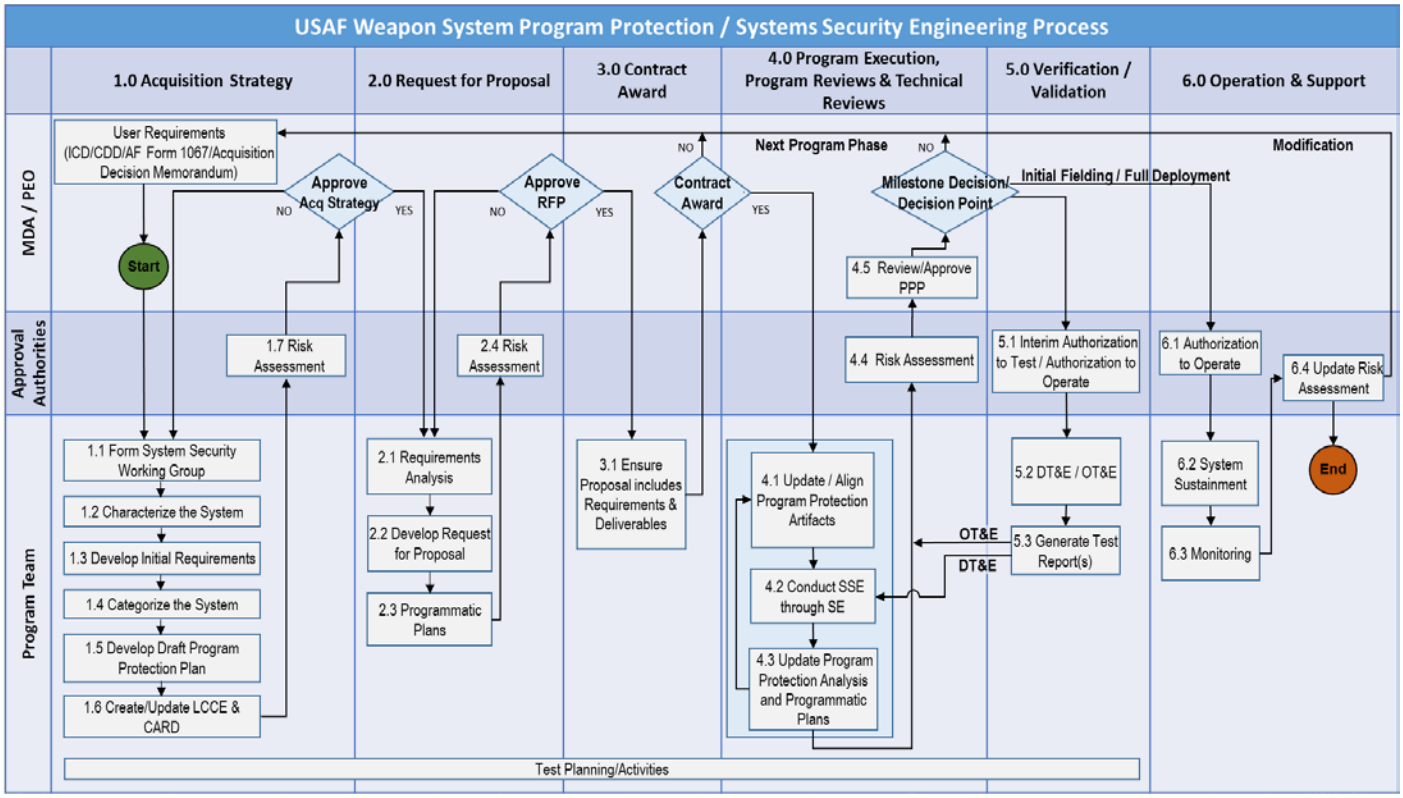


Figure D-1: USAF Weapon System Program Protection/Systems Security Engineering (PP/SSE) Process

Part 1: Aircraft System New Start Program

The first several sections below describe the warfighter's needs and user requirements for the system to be developed from. These are initial inputs developed prior to the program office beginning the PP/SSE Process in Figure D-1 above, and are provided to give context and scope the use case.

Warfighter Statement of Need:

Air Force Intelligence, Surveillance, and Reconnaissance (ISR) operations span all domains— land, sea, air, space, and cyberspace. These operations are undertaken by a variety of platforms—ranging from satellites to RC-135s, JSTARS, U-2s, and unmanned aerial systems (UAS) like Predator and Global Hawk.

Expanding global operations have generated an increased demand for ISR assets.

Mission - Provide 24-hour coverage in an area of interest with high quality sensors while providing a force multiplier, to complement manned/space reconnaissance. Covering the spectrum from peace to war, potential applications of endurance UASs include:

a. Near-Real-Time (NRT) Targeting and Precision Strike Support – offering opportunities to fulfill time-sensitive targeting requirements by providing a means to shorten the targeting cycle for interdiction campaigns through NRT precise location of mobile enemy forces. The ability to locate, identify, and quickly destroy mobile targets will eliminate the enemy's ability to resupply and maneuver forces. Endurance UAS sensor resolution and accuracy will enable expanded use of precision-guided munitions, improving battlefield efficiency.
b. NRT Combat Assessment – providing the battlefield commander with improved situation awareness. Immediate feedback of planned and executed operations will assist with the efficient prosecution of campaigns and minimize the fog and friction of war.
c. Enemy Order of Battle (EOB) – allowing a rapid means to develop and track enemy order of battle information, especially in areas where information is sparse.
d. Battle Damage Assessment (BDA) – providing high resolution, NRT assessment of target damage. Immediate feedback will support the warfighter's immediate restrike requirements.
e. Intelligence Preparation of the Battlefield (IPB) – allowing surveys of areas of interest in preparation for battle or amphibious assaults and landings. Significantly enhances Indications and Warning (I&W) capability.
f. Special Operations support – tracking high-interest, sea-going vessels, high-interest individuals or organizations. UAS information also has the potential of providing direct imagery down links to ground special operations units that need to "look beyond the horizon" for ingress, targeting, or egress from hostile areas.
g. Blockade and Quarantine Enforcement – military and drug enforcement blockade and quarantine missions may be supported by UASs to free up enforcement patrol assets for other missions.
h. Sensitive Reconnaissance Operations (SRO) – supporting missions that , by virtue of collections objectives, means of collection, or area of operations, involve significant military risk or political sensitivity.
i. Humanitarian Aid Missions – providing information on the number of people displaced or survey weather damage, etc.
j. United Nations (UN) Treaty Monitoring – monitoring compliance with UN resolutions, and alerting UN authorities of violations while providing safe and NRT surveillance of areas of interest.
k. Counter Drug Missions – aiding in identification, tracking, and imaging of drug trafficking activities.

l. Single Integrated Operational Plan (SIOP) – assisting missions in support of planning and employment of strategic forces, countering weapons of mass destruction, and nuclear strike assessment.
m. Communications – relaying C4I or other broadcast missions. UASs have potential to significantly enhance Dissemination of Battlefield Intelligence and C2 information to all areas and levels of command.

System-Level Description & Environmental Considerations

Medium Altitude Endurance (MAE) UASs need to provide a broad spectrum of intelligence collection capability to support joint combatant forces in worldwide peace, crisis, and wartime operations. The capabilities of the UAS system will provide for adaptive real-time planning of current operations, to include: monitoring enemy offensive and defensive positions, deception postures and combat assessment. MAE UASs need to provide a rapid turnaround of raw data to aid a robust targeting cycle following a "First Look, First Shoot, First Kill" methodology. The AV needs to be operable in mildly adverse weather, equivalent to instrumented flight by a light civil aircraft. The AV design needs to include inherently low signature characteristics to the maximum extent possible. The MAE UAS platform needs to be able to provide Intelligence, surveillance and reconnaissance (ISR) multi-INT and Suppression of Enemy Air Defenses (SEAD)/Strike missions within the emerging global command and control architecture.

MAE UAS Requirements:

- Low-cost, UAS < $20M
- Range 500 NM (SEAD), Persistence 24 hour (ISR)
- Capable of global day/night deployment and operation in enemy contested environment
    - Autonomous beyond-line-of-sight (BLOS) capability
    - Execute pre-planned missions with in-flight re-tasking effective Battlefield Management
    - Robust and secure command and control (C2) communications, including line-of-site (LOS) and BLOS
- Reconfigurable mission control station for multi-ship UAS operations
- GCS reach-back capability

The AV is limited to operations in mildly adverse weather, equivalent to instrumented flight by a light civil aircraft. Adverse weather conditions, such as icing, moderate to heavy precipitation airborne or on the ground, or high surface winds may prevent or affect launches or operations. Neither the Ground Control Segment (GCS) nor the AV are water-proof. Max crosswind limit is 14kts normal to runway for launch & recovery operations. Maximum ground operation wind limit is 30kts. The AV has no tie down points and must be hangered during high wind conditions. Maximum true airspeed of the vehicle will be exceeded by winds aloft in excess of 110kts. Furthermore, areas of responsibility (AORs) with heavy precipitation seasons and adverse landing conditions may severely impede operations.

High Performance Team (HPT) Activities

As shown in **Figure D-2**, Program Protection/Systems Security Engineering (PP/SSE) Process Flow, the HPT is responsible for user requirements, including the implementation of the Joint Capabilities Integration and Development System (JCIDS) Survivability Key Performance Parameter (KPP 5 in this example) and Cyber Survivability Attributes (CSAs).

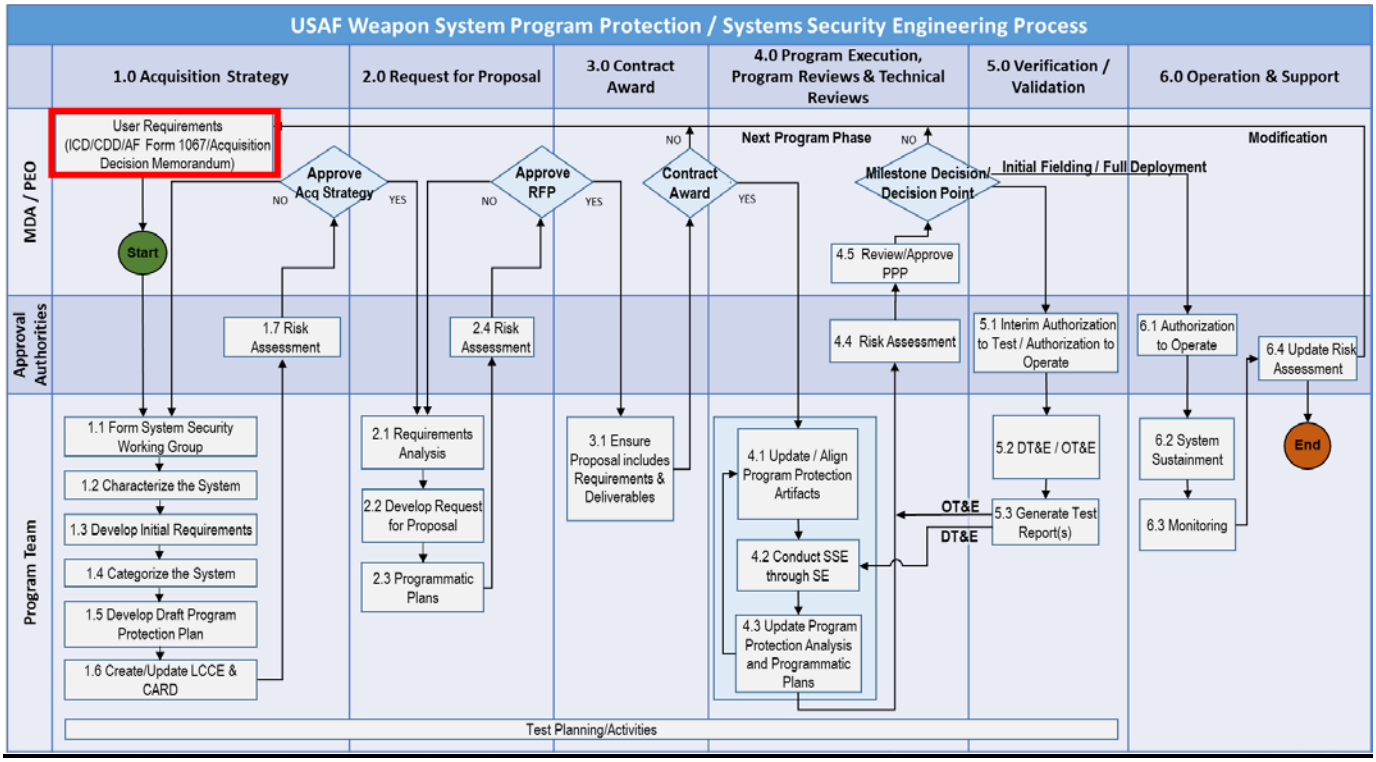


Figure D-2. Program Protection/Systems Security Engineering (PP/SSE) Process - HPT

CDD Requirements (SSE Acquisition Guidebook, para 1.1)

KPP 1 – Autonomous operations BLOS IAW mission plan (Threshold=Objective)

KPP 2 – Manual LOS launch and recovery (Objective); Autoland (Threshold)

KPP 3 – Adaptable Mission Planning/Re-tasking (Threshold = Objective)

KPP 4 – Multi-ship Mission Control Station (Threshold=Objective)

KPP 5 – System Survivability (SS): The system shall be able to maintain critical capabilities under applicable threat environments. (Threshold=Objective)

KPP 6 – Weapons load outs (Threshold=Objective)

KPP 7 – Battle field situational awareness with Multi-INT capable sensor suit – Infrared Search and Track (IRST), Synthetic Aperture Radar (SAR), and Ground Moving Target Indication (GMTI) (Threshold=Objective)

KSA 1 – Fly away cost < $20M

KSA 2 – Deployment footprint 2 C-130 or 1 C-17

KSA 3 – Multi-spectral sensor pod carriage

Weapon System High Priority Missions

The UAS will have two primary mission areas, each having multiple types of missions, some of which are high priority missions. KPPs 1, 2, and 5 and KSAs 1 and 2 support all missions. The remaining KPPs / KSAs support individual missions as listed below:

1. Intelligence, Surveillance, and Reconnaissance (ISR) operations
    a. *Dissemination of Battlefield Intelligence**
    b. *Special Operations Support**
    c. *Battle Damage Assessment (BDA)**
    d. Blockade and Quarantine Enforcement
    e. United Nations (UN) Treaty Monitoring
    f. Humanitarian Aid Support
    g. Border Control and Drug Enforcement
    h. *NBC Treaty Compliance Monitoring**
2. Suppression of Enemy Air Defenses (SEAD) / Near-Real-Time (NRT) Strike
    a. *Special Operations Support**
    b. *NRT Combat Assessment**

**These missions have been identified as highest priority by Warfighter*

This Program Protection Use Case exercise focuses on the Functional Thread Analysis (FTA) of two of these priority missions shown in **Figure D-3**.:

1) Dissemination of Battlefield Intelligence
2) NBC Treaty Compliance Monitoring

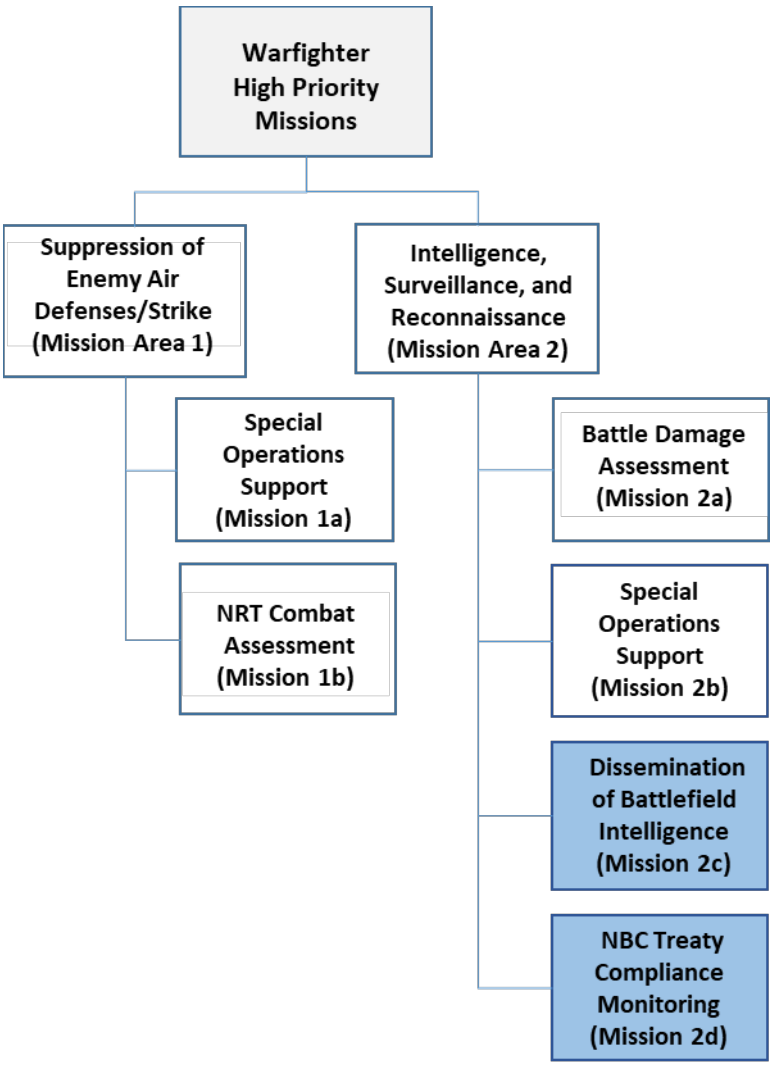


Figure D-3. MAE UAS High Priority Missions

For the ISR mission **(Figure D-4)**, Dissemination of Battlefield Intelligence involves mission/flight planning, LOS launch of the UAS, BLOS control & navigation up to 500NM to the target area, loiter and collect, analyze, and disseminate intelligence for up to 24 hours, BLOS control & navigate back to the point of origin, LOS descent & landing, conduct post flight activities. This mission depends on a number of essential functions, systems, and components, as well as LOS C-band data link, Ku-Band Satellite link, UHF/VHF voice coordination with airspace control authorities, differential Global Positioning System (GPS), and multi-spectral sensors for treaty compliance monitoring. Essential sensors for the Dissemination of Battlefield Intelligence mission are Electro-Optic/Infrared (EO/IR), Synthetic Aperture Radar (SAR), and signals intelligence (SIGINT). The mission of NBC Treaty Compliance Monitoring depends on the same processes, functions, systems, and components, with the exception of having different essential sensors. Essential sensors to support the NBC Treaty Compliance Monitoring mission are the Multi-Spectral Sensor Pod and the EO/IR sensor.

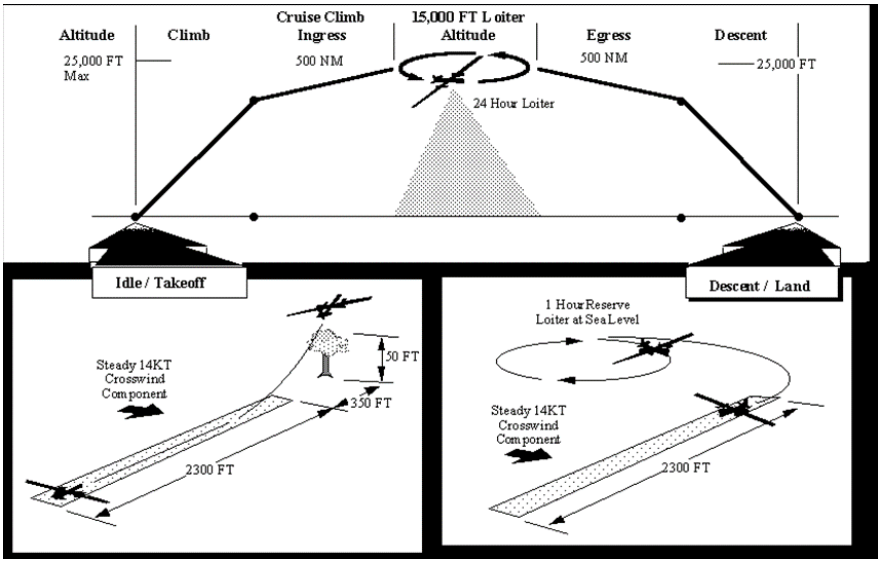


Figure D-4. Intelligence, Surveillance, and Reconnaissance (ISR) operations

Figure D-5 is a notional concept of operations (CONOPS) for battlefield communications and data dissemination. As can be seen the UAS includes communications with a number of external systems in order to perform various missions, using the C-band data link for LOS operations, and a wideband Ku-band data link for over the horizon operations. The UHF SATCOM is seldom used due to its low data transfer rate. All data links provide command and control uplinks as well as imagery and telemetry downlinks.

The GCS will employ tactical radios for Joint Forces Commander (JFC)/Joint Force Air Component Commander (JFACC) tasking and support from the Component Commander responsible for administrative support to the MAE UAS detachment. The GCS is linked to a TROJAN SPIRIT II (TS II) trailer, capable of SATCOM relay, and linked to Joint Deployable Intelligence Support System (JDISS) via Joint Worldwide Intelligence Communications System (JWICS) connectivity in the TROJAN SPIRIT network. The TS II is an Army satellite communications terminal and system which provides access to intelligence dissemination and processing systems. It provides both Secure Compartmented Information (SCI) and collateral circuits over C or Ku Bands.

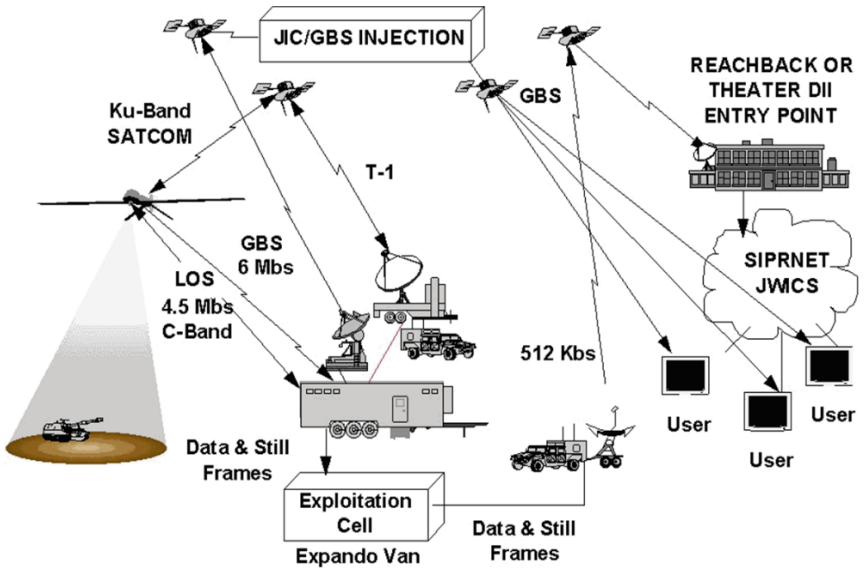


Figure D-5. External Communication CONOPS for MAE UAS

Function	Connection	Via	Frequency	Data Rate	Relevant Mission
Mission Tasking (Air Tasking Order)	Air Operations Center (AOC)	Voice, Data (AUTODIN)	-	1.2/2.4 Kbs	1a, b, c, d, e, f, g, h; 2a, b
Dynamic Tasking	AOC	Voice	UHF	-	1a, b, c, g; 2a, b
Situational Awareness	AOC, Combined Tactical Operations Center (CTOC), Marine Air-Ground Task Force (MAGTF)	TRIXS/TRAP, TADIX-B, TIBS	UHF - MILSAT	-	1a, b, c, e, g, h, 2a, b
Airspace Management, SOF	Airspace Control Authority (ACA)/Area Air Defense Commander (AADC), Air Traffic Control (ATC)/JRC	Voice	VHF/UHF - MILSAT	-	1a, b, c, d, e, f, g, h; 2a, b
Tactical Reporting	Joint Task Force (JTF), AOC, Units	Voice, Data (AUTODIN)	UHF - MILSAT	1.2 to 4.8 Kbs	1a, b, c, d, g; 2a, b
Video Dissemination	Exploitation Sites	TROJAN SPIRIT II JDISS/JWICS GBS/JBS	Ku/C/X Band - COMSAT, DSCS	512 Kbs to 6 Mbps	1a, b, c, d, e, f, g, h; 2a, b
Frame Dissemination	Exploitation Sites	JDISS/JWICS/SIPRNET GBS/JBS	Ku/C/X Band - COMSAT, DSCS	512 Kbs to 6 Mbps	1a, c, e, g; 2a, b

Functional Thread Analysis (FTA)

Once the initial weapon system requirements are defined by the HPT, the Program Office team begins a Functional Thread Analysis (FTA).

System Characterization and Categorization

The first step in the FTA is to conduct a functional decomposition to identify critical AV and GCS components and Critical Program Information (CPI) as shown in **Figure D-6** below.

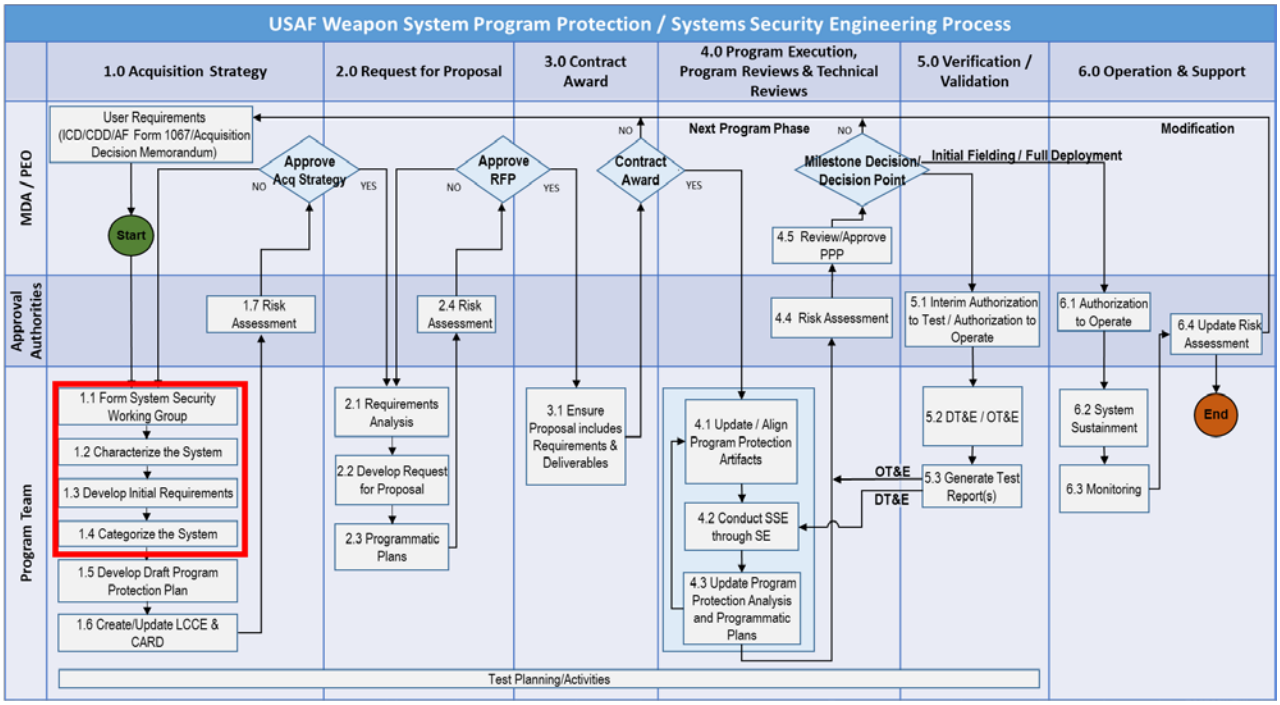


Figure D-6. PP/SSE Process – System Characterization / Categorization and Initial Requirements

Based on the CONOPS discussed above, the initial system boundaries can be developed. The security boundary can be depicted as a notional boundary between the UAS segments and the external security environment associated with it. This includes persons, external systems, and interactions with the UAS including maintenance and supply chain activities.

Internal Connectivity - For the UAS internal connectivity consists of analog and discrete I/O, bi-directional serial data busses (e.g., MIL-STD-1553, ARINC 429, RS-232, Ethernet) and some parallel data bus communications (e.g. PCI) as well as NIPRNet, SIPRNet.

External Connectivity:

- External AV Segment connectivity requirements includes commercial SATCOM, INMARSAT, Link-16, GPS, Military SATCOM, VHF/UHF, SAP/JWICS, Common Data Link (CDL), etc.
- External GCS Segment connectivity adds NIPRNet, SIPRNet, SAP/JWICS, Cross-domain data transfer to/from those networks, and 802.11 Wireless

Technical Exposure - adversary's understanding of and access to the system's hardware and software intellectual property in order to identify and exploit vulnerabilities is/or should be limited by Controlled Unclassified Information (CUI) processes and procedures. See SOW language (Attachment D-1).

Assumptions regarding "untrusted" interactions:

- Personnel interactions (operators, maintainers, developers) are considered trusted because of physical security provisions assumed to be in place. That doesn't preclude unintentional security vulnerabilities associated with personal electronic devices (PED) with access to the internet as an example.
- GPS, SATCOM, ILS, ATC and other sources of NAS data are assumed trusted; communication links are considered vulnerabilities, however.
- Defense Intelligence Agency Threat Assessment Center (DIA TAC) - DoD has designated the Defense Intelligence Agency (DIA) to be the DoD enterprise focal point for intelligence and counterintelligence assessments of supplier threats to acquisition programs providing critical weapons, information systems, or service capabilities.
- Safety critical developmental processes are utilized to provide reduction in vulnerability risks due to untrusted interactions; for example, levels of rigor assignments to safety critical software
- Anti-tamper implementations to protect Critical Program Information (CPI) and Critical Components (CC) are leveraged to bake in cybersecurity resiliency.

The MAE UAS security boundary is shown in **Figure D-7**.

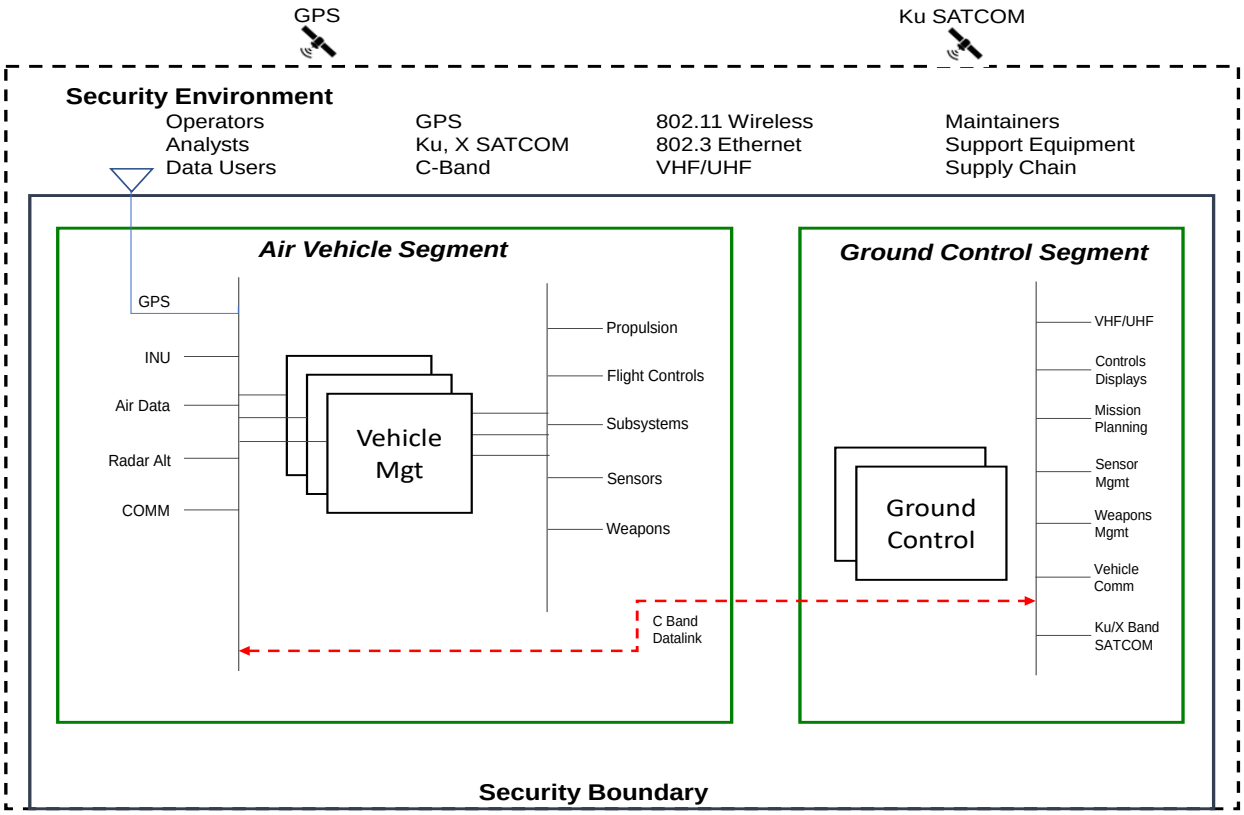


Figure D-7. MAE UAS Security Boundary

Cyber Survivability Endorsement (CSE) & Cyber Survivability Attributes (CSA) (SSE Acq Guidebook, para 1.1.1)

Objective of the CSE Process: Ensure cyber survivability requirements are articulated sufficiently to ensure that Joint Warfighting Systems are designed to prevent, mitigate and recover from cyber-attacks; from the beginning at requirements definition and throughout their lifecycle by applying a risk managed approach to building and maintaining systems.

Step 1 – Determine the Mission Type (MT) of the System. Both the Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring missions are Operational/Tactical Missions (MT 3). Weapon system degradation would result in high risks to mission completion, requiring unique protections and a focus on survivability and resiliency requirements that will ensure their continuous operation.

Step 2 – Determine the Cyber Dependency Level (CDL) of the System. Our cyber dependency is based on the system's degree of connectivity and technical exposure. For our UAS example, the CDL has been determined to be High (CDL 3).

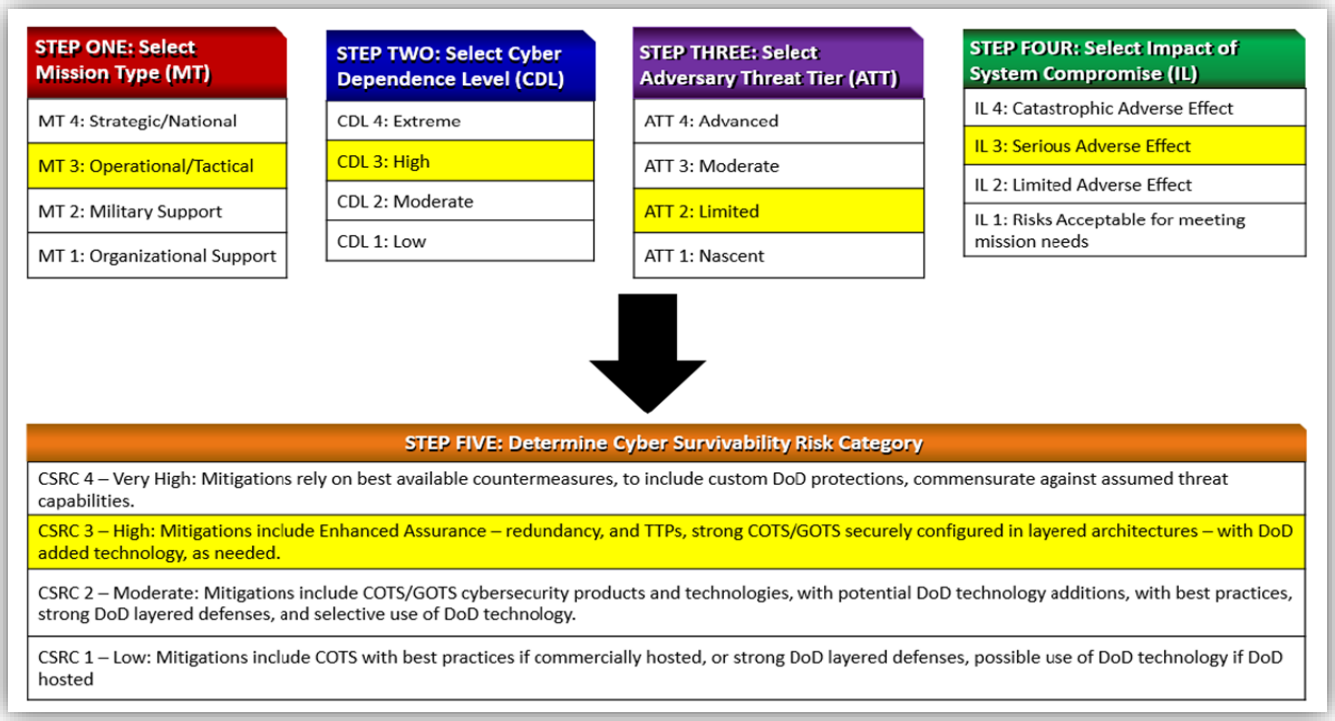
Step 3 – Determine the Adversary Threat Tier (ATT) to the System. Our threat environment is described as Limited (ATT 2), i.e. able to identify and target – for espionage or attack – easily accessible unencrypted networks running common operating systems using publicly available tools.

Step 4 – Determine the Impact Level (IL) of System Compromise to the Mission. In relation to both the Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring missions, a compromise of the MAE UAS would result in a Serious Adverse Effect (IL 3) – an unacceptable compromise of mission capability or significant mission degradation.

Step 5 – Determine the Cyber Survivability Risk Category (CSRC) of the System. Applying the High Water Mark (HWM) method to the MT, CDL, ATT and IL determined above, the CSRC for both the Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring missions is High (CSRC 3). For a CSRC 3, the CSE Implementation Guide (CSEIG) recommends including requirements to:

- Prevent cyber-attacks 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 & Harden Cyber Attack Surfaces; Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds.
- Mitigate the effects of cyber-attacks: Baseline & Monitor Systems and Detect Anomalies; Manage System Performance if Degraded by Cyber Events; Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds.
- Recover from cyber-attacks: Recover System Capabilities; Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds

Table D-1. UAS Cyber Survivability Risk Category



Per CSEIG Vol I, appropriate CSAs must be identified and tailored for system-specific implementation and updated threat; testable and measurable in relevant environment for DT&E in support of system verification of derived cyber survivability requirements and operational assessments of cyber survivability capability requirements. The Cyber Survivability Attributes to be applied to the system's high priority missions have been identified by the High-Performance Team (HPT) and tailored as shown in **Table D-2** below

Rationale is provided for applicability of each attribute for each mission (Dissemination of Battlefield Information and NBC Treaty Compliance Monitoring). Mitigations in some instances, e.g. CSA 07, are inherent in the design used to support the NBC Treaty Compliance Monitoring mission. Applicability of each CSA should be assessed for all other missions. (SSE Acq Guidebook, para 1.1.2)

Table D-2: User Tailored Cyber Survivability Attributes

CSA	Pillar	Cyber Survivability Attribute (CSA) **Need to be tailored**	Dissemination of Battlefield Information		NBC Treaty Compliance Monitoring	
			Applicable to the AV Segment (Yes/No)	Applicable to the GCS (Yes/No)	Applicable to the AV Segment (Yes/No)	Applicable to the GCS (Yes/No)
CSA 01	Prevent	The system ensures that only identified, authorized and approved persons and non-person entities are allowed access or interconnection to the system.	**No** Physical security controls (guards, gates, accesses) in place for AV prevent the need for further dedicated controls for CSA 01.	**Yes**	**No** Physical security controls (guards, gates, accesses) in place for AV prevent the need for further dedicated controls for CSA 01.	**Yes**
CSA 02	Prevent	Wireless and wired signaling and communications should not compromise OPSEC.	**Yes**	**Yes**	**Yes**	**Yes**
CSA 03	Prevent	All intelligence dissemination transmissions and communications shall be maintained at the appropriate security level (e.g. secret, top secret, TS-SCI).	**Yes**	**Yes**	**Yes**	**Yes**
CSA 04	Prevent	The system defends against adversary attempts to exploit information resident in the system. The system counters attempted malicious data injection, other corruption, or denial of service activities. The system also protects information at rest, against corruption, exploitation or exfiltration.	**Yes**	**Yes**	**Yes**	**Yes**
CSA 05	Prevent	The system's safety and mission critical functions are isolated from less critical functions.	**Yes**	**Yes**	**Yes**	**Yes**

CSA	Pillar	Cyber Survivability Attribute (CSA) **Need to be tailored**	Dissemination of Battlefield Information		NBC Treaty Compliance Monitoring	
			Applicable to the AV Segment (Yes/No)	Applicable to the GCS (Yes/No)	Applicable to the AV Segment (Yes/No)	Applicable to the GCS (Yes/No)
		The system preserves minimum essential performance for mission critical and supporting platform functions.				
CSA 06	Prevent	Minimize and Harden Cyber Attack Surfaces	**Yes**	**Yes**	**Yes**	**Yes**
CSA 07	Mitigate	The system monitors for cyber anomalies (e.g. leaks, intrusions, and attack effects) in critical functions, components, and communications. The 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. The system logs all cyber anomalies in non-volatile memory.	**Yes**	**Yes**	**Yes** However, mission does not drive additional mitigations to cyber vulnerabilities beyond the mitigations in place for other priority missions.	**Yes** However, mission does not drive additional mitigations to cyber vulnerabilities beyond the mitigations in place for other priority missions.
CSA 08	Mitigate	No single failure results in the inability to complete the mission(s).	**Yes**	**Yes**	**No** NBC Multi-Spectral Sensor Pod does not incorporate redundancy. If sensor fails, mission is terminated.	**Yes**
CSA 09	Recover	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.	**Yes**	**Yes**	**No** NBC Multi-Spectral Sensor Pod does not incorporate redundancy. If sensor fails, mission is terminated.	**No** Loss of Ground Station real time monitoring backed up by sensor pod data recorder.
CSA 10	Prevent Mitigate Recover	Actively Manage System's Configuration to Counter Vulnerabilities at rest, prior to and during all mission phases.	**Yes**	**Yes**	**Yes**	**Yes**

Initial Functional Thread Analysis (SSE Acq Guidebook, para 1.1.2)

During the development of the CDD requirements, the High-Performance Team (HPT) completed a functional decomposition analysis to understand mission functional threads. These functional elements were mapped to Mission Critical Functions (MCFs), Flight/Safety Critical Functions (SCFs), and functions associated with Critical Program Information (CPI). The warfighter community provided inputs during the HPT on which Cyber Survivability Attributes (CSAs) are applicable to achieve the SS KPP.

AV critical functions are defined in three categories: Safety, Flight, and Mission.

Safety Critical – A condition, event, operation, process, or item whose mishap severity consequence is either Catastrophic or Critical (Ref. MIL-STD-882) (i.e., safety critical function, safety critical path, safety critical software, or safety critical component).

MIL-HDBK-516C Section 15 and Airworthiness Circular (AWC) 17-01 identify the artifacts and activities associated with the identification of Safety Critical Functions and systems.

The safety critical category is a broader definition of the categorizations of safety and includes flight critical but may not be limited to controlling flight.

Flight Critical - A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to achieving or maintaining controlled flight of an aircraft.

Mission Critical - Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed (Ref. DoDI 5200.44).

The warfighter has identified two mission areas, Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring, each containing several high priority missions **(Figure D-3)**. These missions directly support **KPPs 1, 5, 6, and 7 and KSA 3 (NBC Treaty Compliance Monitoring only)**. Those mission areas and high priority missions can be decomposed into the essential functions required in the UAS to accomplish them.

A continuation of the FTA is to examine the functions to ensure they were appropriately identified as flight/safety/mission critical in accordance with MIL-STD-882E. Functional decomposition can be accomplished using the methodology described in USAF Airworthiness Circular (AW) 17-01. **Figure D-8** shows the initial decomposition of the functional threads for the Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring missions, highlighted. The colors in the figure designate whether the function is located in the AV segment (Blue), GCS (Green) or spans the two (Gradient).

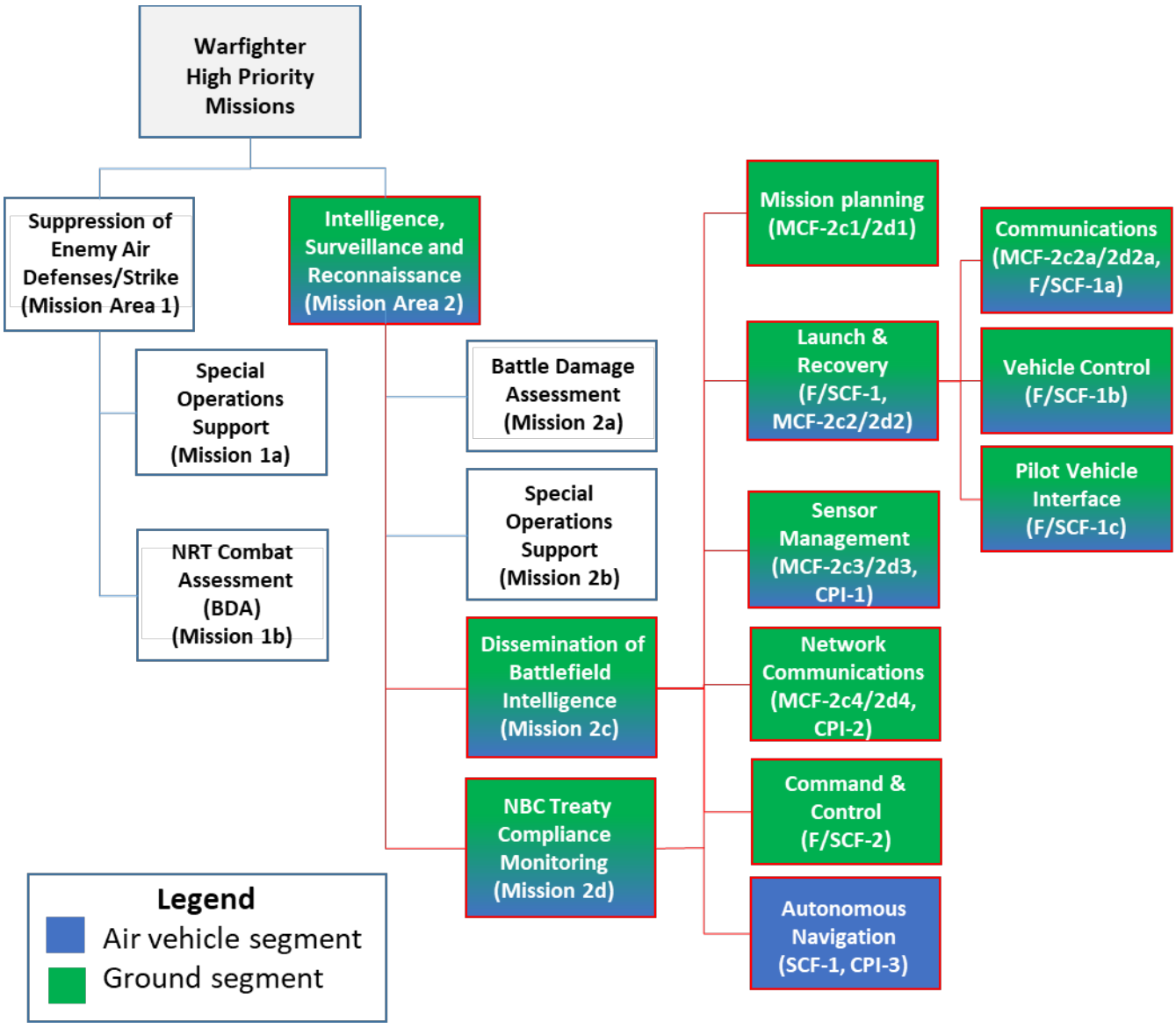


Figure D-8. Initial ISR Functional Thread for Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring

Conduct CPI Identification/ Analysis (SSE Acq Guidebook, para 1.2.1)

One of the most important steps in the FTA process is the identification of CPI and Critical Components (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 Systems Security Engineering (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. Identification of CC/CPI follows the process as outlined in

Step 2 of the United States Air Force Combined Process Guide for Critical Program Information (CPI) and Critical Component (CC) Identification, dated 8 May 2018.

Critical functions defined in **Table D-3** are designated as MCF-xx for Mission Critical, F/SCF-xx for Flight Critical, and SCF-xx as Safety Critical. Initial CPI analysis identifies those critical functions in **Table D-3** as CPI-xx.

For this example, Flight / Safety Critical subsystems are identified as Communication, Vehicle Control, Autonomous Navigation, Command and Control, and Pilot Vehicle Interface, as shown in **Table D-3**.

For this example, specific CC/CPI are identified in the Sensor Management, Autonomous Navigations, and Network Communications subsystems, as shown in **Table D-3**.

Table D-3. Initial Weapon System Criticality and CPI Identification

Mission	Critical Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I,II,III,IV)
Dissemination of Battlefield Intelligence AND NBC Treaty Compliance Monitoring	Mission Planning (MCF-2c1/2d1)		I
	Communications (F/SCF-1a, MCF-2c2/2d2)		I
	Vehicle Control (F/SCF-1b)		I
	Pilot Vehicle Interface (F/SCF-1c)		I
	Sensors (MCF-2c3/2d3; CPI-1)		II
	Network Communications (MCF-2c4/2d4, CPI-2)		I
	Command and Control (F/SCF-2)		I
	Autonomous Navigation (SCF-1; CPI-3)		I

TO BE COMPLETED PRIOR TO PDR

Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible

Develop Initial System Requirements (SRD) (SSE Acq Guidebook, para 2.2)

The system-level SSE requirements applicable to Mission 2c (Dissemination of Battlefield Intelligence), based on the HPT identified CSAs, are found in **Table D-4**. Each recommended requirement was assessed for both the AV and GCS elements of the UAS. See embedded worksheet for content, rationale for tailoring, and initial verification requirements.

System Requirements

These requirements were tailored to align with the program definition. As an example, recommended requirement 8.2 (The system shall provide capabilities to shed non-mission critical functions, systems/sub-systems, and interfaces) was deleted as there were no non-mission critical functions identified.

Another example of tailoring is system requirement 5.2 (The system shall ensure safety critical and mission critical functions are prioritized appropriately to ensure mission completion). This requirement was deleted as it is addressed through the systems engineering controls for safety critical functions required by MIL-HDBK-516C and Airworthiness Circular 17-01 requiring Safety Critical Functional Thread Analysis (SCFTA). Integration testing at all levels as well as rigorous Failure Modes and Effects Testing (FMET) verifies these controls.

Table D-4: System-Level SSE Requirements Applicable to Mission 2c: Dissemination of Battlefield Intelligence

Requirement	System Specification Requirements (Tailored for UAS)
Prevent	**CSA 01 - Control Access**
1.1a	The system shall ensure that the Ground Control Segment is accessed only by authenticated persons and authenticated external interconnections to the system or internal interconnections with sub-elements within the security boundary.
1.1b	The system shall ensure that the Air Vehicle is accessed only by authenticated persons and authenticated external interconnections.
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 IAW MIL-STD-464, paragraph 5.14.
2.2	The system shall minimize wired and wireless signals to generate and upload mission plans in accordance with Emissions Control (EMCON), using AFGSCI 10-707 as guidance.
Prevent	**CSA 03 - Secure Transmissions and Communications**
3.1	The system shall encrypt all data link transmissions and communications of data in transit external to the Air Vehicle and Ground Control Segments at the appropriate classification levels.
Prevent	**CSA 04 - Protect System's Information from Exploitation**
4.1	The system shall ensure information integrity and system performance sufficient to complete priority missions after any single cyber event.
4.3	The system functions containing critical program information (CPI) shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.
4.4	The system shall implement sanitization processes to protect CPI in all phases of mission execution.
Prevent	**CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels**
5.1	The system shall isolate mission critical and safety critical CPI functionality from less critical functions.

Requirement	System Specification Requirements (Tailored for UAS)
Prevent	**CSA 06 – Minimize and Harden Attack Surfaces**
6.1	The system shall configure external interfaces to perform safety critical and mission critical functions.
6.2	The system shall ensure interfaces are hardened, while supporting safety/mission critical functions.
Mitigate	**CSA 07 – Baseline & Monitor Systems and Detect Anomalies**
7.1	The system shall monitor operational parameters, boundaries, and configuration controls.
7.2	The system shall analyze performance through a baseline comparison to detect anomalies and attacks.
7.3	The system shall generate and store mission logs.
Mitigate	**CSA 08 - Manage System Performance if Degraded by Cyber Events**
8.1	The system shall alert users of detected anomalies and attacks.
8.3	The system shall maintain mission critical functions in a cyber contested operational environment during/after observed anomaly(ies).
8.4	The system shall maintain safety and mission critical functions in a cyber-contested operational environment during/after observed anomalies.
8.5	No single cyber related failure shall result in the inability to complete the mission.
Recover	**CSA 09 - Recover System Capabilities**
9.1	The system shall provide the capability to recover to a known operating 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 scans shall have the capability to be updated to ensure appropriate, applicable requirements are captured (e.g., STIGS, SRG, Benchmarks, Hardware and Firmware versions, etc.) for: (a) hardware, (b) software, and (c) firmware

Identify Initial Vulnerability & Threats (SSE Acq Guidebook, para 1.10)

After development of initial weapon system requirements (System Requirements Document – SRD), an initial vulnerability and risk assessment was conducted **(see Figure D-10)**.

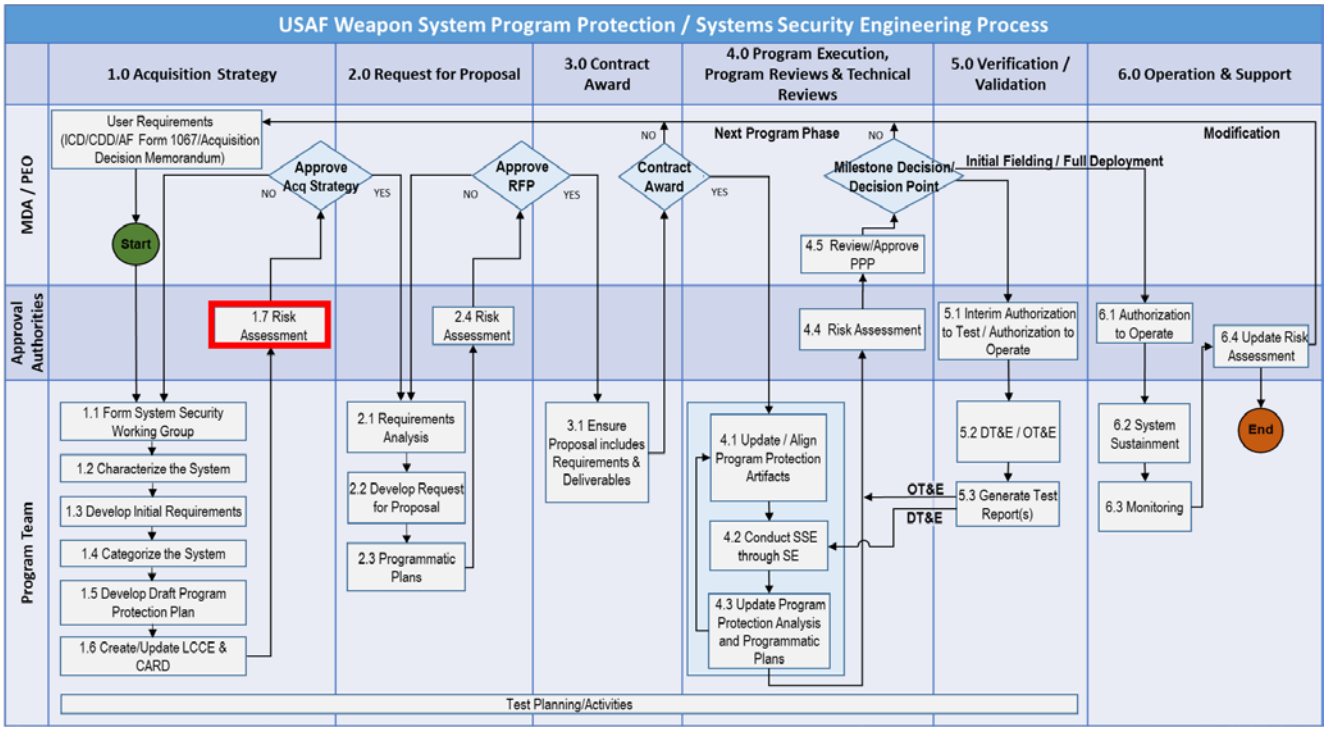


Figure D-9. PP/SSE Process – Initial Risk Assessment

Considering security boundaries the initial UAS vulnerabilities includes:

- Personnel involved in development, operation, maintenance & repair, and updates of the UASs and components (These are assumed trusted for intentional cyber-attacks based on Weapon System security plans, processes, and procedures)
- Foreign actors with malicious intent (Limited vulnerability based on Technical Data being CUI)
    - Spoofing (imitating its characteristics)
    - Man-in-the-middle (captures and relays and potentially alters the C2 data)
    - Denial of Service (make the C2 data unavailable)
    - Replay Attacks (maliciously repeated or delayed)
    - Relay Attacks (captures and relays)
- Data links subject to hacking (C-band data link)
    - Inject Unexpected Items
- Code Injection
    - Command Injection
    - Fault Injection
    - Manipulate Vehicle Control, Timing and States
- Wireless communications
    - Code Injection
    - Command Injection
    - Fault Injection

Using the methodology depicted in **Figure D-10** from Appendix A: USAF SSE Acquisition Guidebook Section 1.10, the initial unmitigated risk to the UAS can be identified.

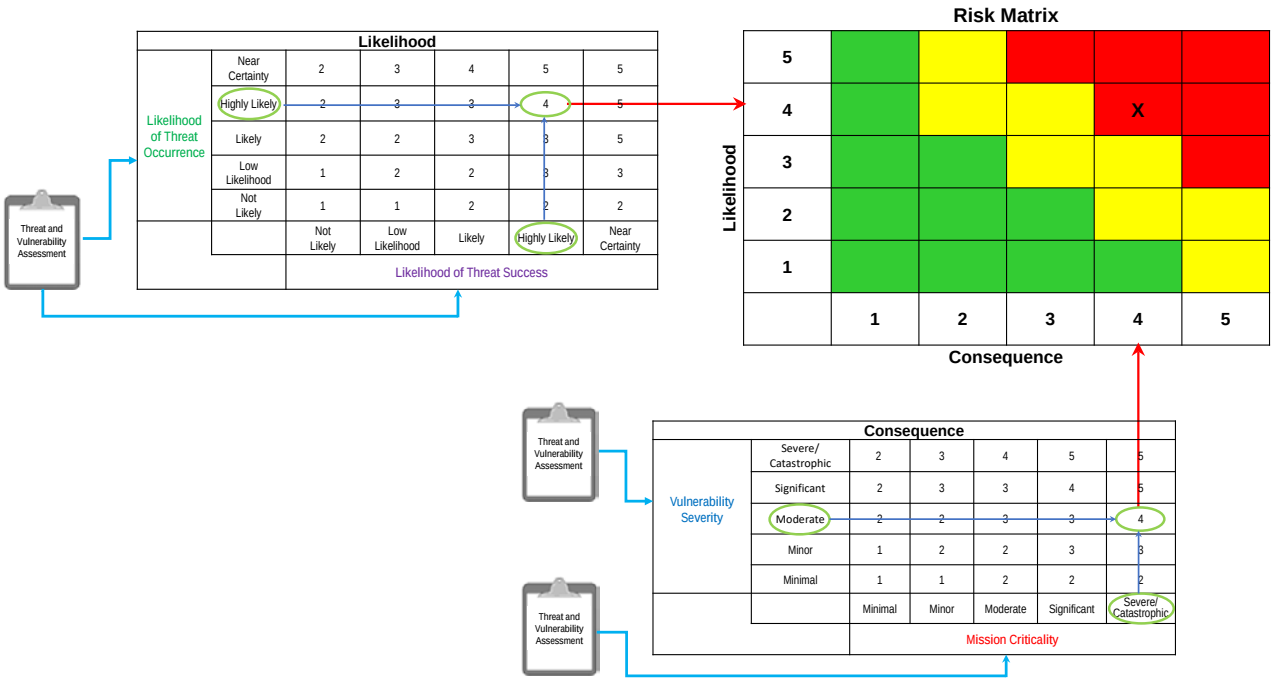


Figure D-10. USAF SSE Acquisition Guidebook, Section 1.10 Risk Management

Applying the methodology above, the unmitigated risk to Mission 2c (Dissemination of Battlefield Intelligence) based on the initial analysis is shown in **Figure D-11** below.

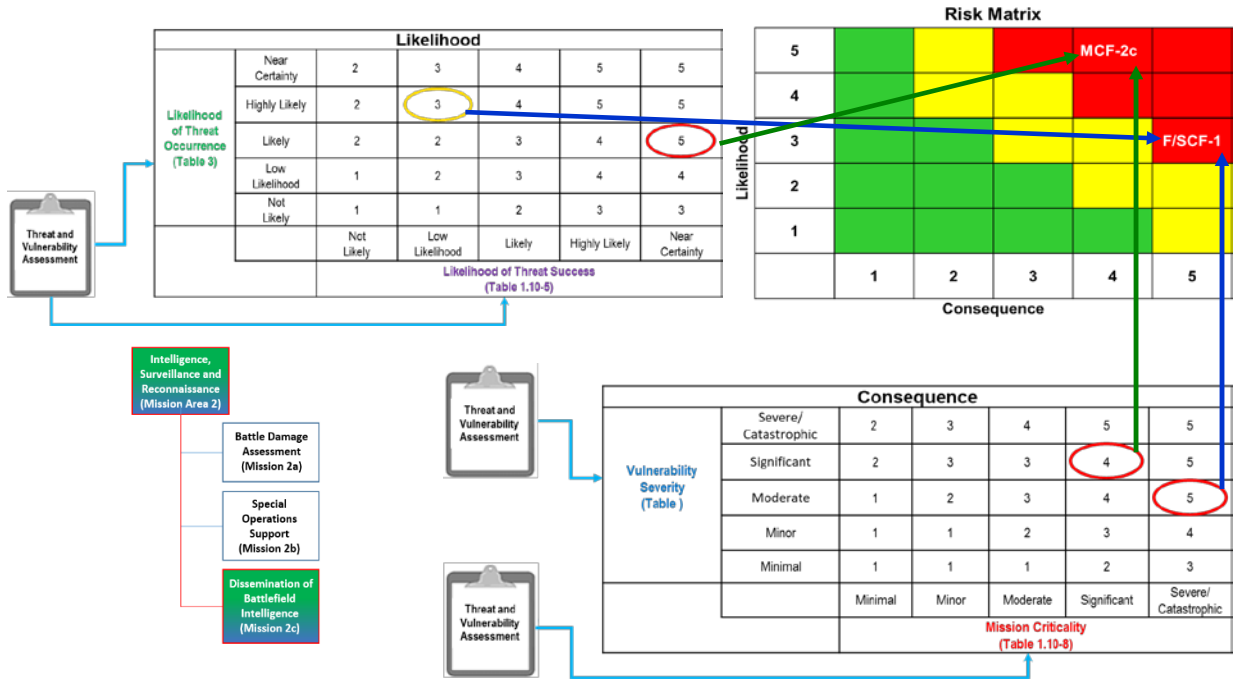


Figure D-11. Initial Unmitigated Risk Assessment (Mission 2c: Dissemination of Battlefield Intelligence)

Requirements Analysis (SSE Acq Guidebook, para 2.2)

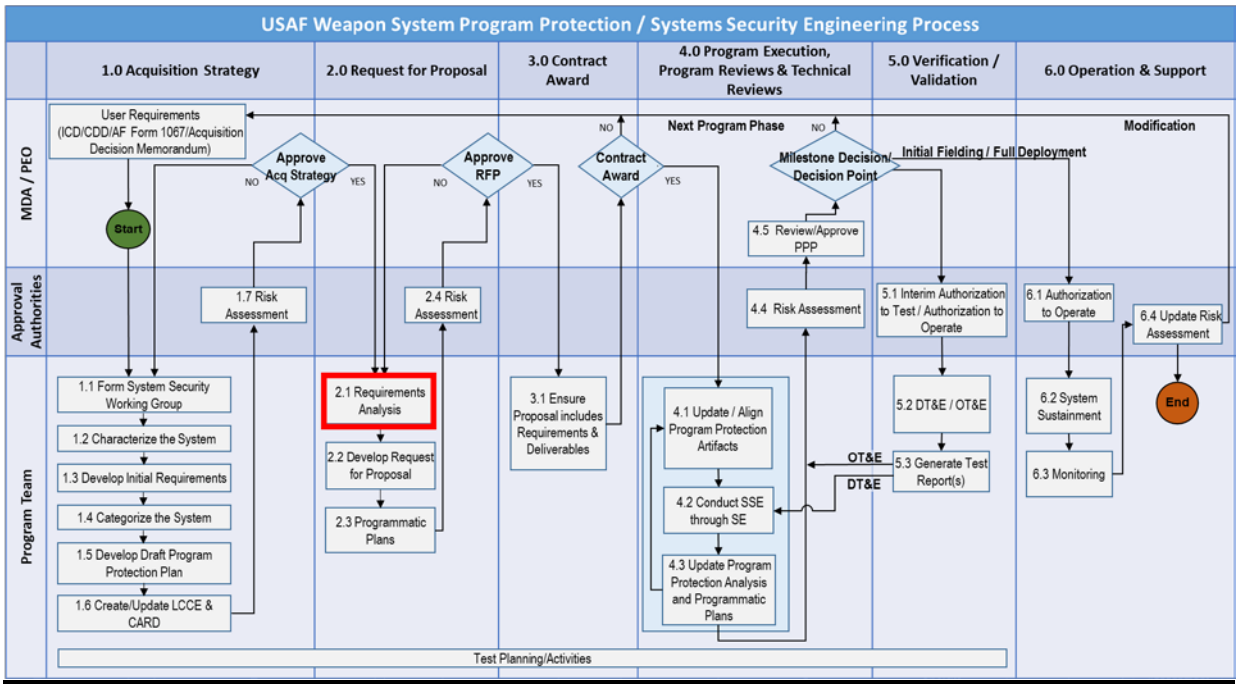


Figure D-12. PP/SSE Process – Requirements Analysis

Requirements analyses are conducted to ensure the correct and relevant requirements are selected, including tailoring, for the UAS. Listed below are some considerations used during the UAS requirements analysis. The numbered requirements referenced below can be found in the System Requirements spreadsheet embedded earlier in this document in Attachment 1 to Appendix A: USAF SSE Acquisition Guidebook Table 2.2-1.

- Since the AV segment is unmanned, requirements 1.1 and 1.2 may only apply to the GCS. That might be overstating the case since the AV Segment requires scheduled and unscheduled maintenance and periodic HW/SW updates to on-board systems. The thought is the aircraft would be protected by guards, gates, and guns and therefore not appropriate for the SRD. The GCS would certainly employ authentication and least privilege access more appropriate for SOW and Security Plan. See Attachment D-1 for SOW language and Attachment D-2 for CDRLs.
- All safety/mission critical hardware elements are qualified to the EEE requirements in MIL-STD-464, including TEMPEST, EMCON (2.1), HERO, HERF and HERP. This is an area where the threat and attack path must be identified to determine if standard design practice is deficient.
- For MCF-2c, wireless connections can be controlled via EMCON procedures in the mission plan and encrypted data links. For F/SCF-1, wireless connections are limited to encrypted C-band and UHF/VHF radio Communications. The radios are functionally isolated from the Launch and Recovery function thread. (requirements 2.2 and 3.1)
- MCF-2c, F/SCF-1, and F/SCF-2 shall embody the design best practices identified in JSSG2005, JSSG 2008, Mil-HDBK-516C, and FAA AC 25.1309-1A:
    - Requirement 4.1 - Information integrity and performance is ensured by the HW/SW development processes applied to safety critical components supporting the SCF [e.g. USAF AC17-01, DO-178C]. Pre-flight and/or pre-engagement built-in-test (BIT) ensures the system and all redundant elements are performing within acceptable tolerance levels. Monitoring redundant elements of the SCF in-flight protects against anomalous behavior

unless the attack can create the same effects in multiple, redundant, and isolated elements simultaneously (common mode). Some common mode protection is provided by watch dog timers (WDT), which trigger a warm restart and initialize all input data to a predetermined value, if a process times out. [JSSG 2008, Mil-HDBK-516C]

- Requirement 4.3 - All weapon system components containing CPI require the appropriate anti-tamper provisions. Configuration identification numbers are compared against the released weapon system configuration during maintenance, as well as during start-up and initiated BIT for SCF components. Cyclic Redundancy Checks and checksums also used to detect incorrect software versions and memory anomalies during BIT. [JSSG 2008, Mil-HDBK-516C]
- Requirement 5.1 - Isolating redundant elements in safety/mission critical functions is "best practice" for military and commercial systems. Isolating SCF, components, and wiring from less critical functions is standard practice. Partitioning is also standard practice for software components of varying criticality. [JSSG 2005, JSSG 2008, Mil-HDBK-516C]
- Requirement 5.2 - Prioritization of MCF/SCF based on failures is addressed in JSSG 2008 and Mil-HDBK-516C.
- Requirements 6.1 and 6.2 - Interfaces will be monitored in accordance with requirement 7.1 and encrypted in accordance with requirement 3.1.
- Requirements 7.1 to 7.3 - Monitoring, detection, and annunciating failures and/or anomalous behavior are required for all military and commercial MCF/SCF. Logging the failures is typically done in non-volatile memory internal to the system for retrieval post flight and/or on a data recorder function or maintenance system. [JSSG 2008, Mil-HDBK-516C, AC 25.1309-1A]
- Requirements 8.1, 8.4 and 8.5 – Accomplished thorugh fail-safe design practices identified in JSSG 2008, Mil-HDBK-516C, AC 25.1309-1A
- Requirement 9.1 - This is addressed as part of the FTA, which includes the SCFTA, Safety Hazard Analysis, Failure Modes and Effects Criticality Analysis (FMECA) and resulting Failure Modes and Effects Testing (FMET).
- Requirement 10.1 will need to be incorporated into the Tech Data to ensure continuous monitoring throughout the life cycle.

Note: The requirements analysis could go into greater detail of the specific "best practices" to address the top-level requirements and also address specific attack path items listed above (for example timing and state attacks can be addressed by deterministic processing/execution, device status tables, etc).

This analysis supports the validation of the SRD defined earlier as a key element to the RFP.

Request for Proposal and Planning (SSE Acq Guidebook, para 2.2, 2.3, 2.3.1, 3.1, 3.2, 3.3)

Figure D-13. PP/SSE Process – Develop Request for Proposal

The proposal will contain program protection elements across most sections to include the System Requirements Document (SRD), Statement of Work, Contract Data Requirements List (CDRL), Contract Clauses and Sections L & M.

- The SRD contains the program protection requirements that were developed and analyzed in the Develop Initial System Requirements (SRD) section above (see the system level requirements in the embedded worksheet in this section, and reference SSE Acq Guidebook, para 2.2).
- A security classification guide needs to be developed and approved for collateral and higher levels, if required (See Attachment D-4 Section L and M language). (SSE Acq Guidebook, para 2.3.1)

- As the Statement of Work is developed, the program protection elements identified in Attachment D-1 need to be considered for inclusion along with the associated CDRLs (provided in Attachment D-2. (SSE Acq Guidebook, para 2.3)
- The main body of the contract needs to include the contract clauses addressed in Attachment D-3 (SSE Acq Guidebook, para 3.1)
- The RFP will include instructions to the offeror (Section L) as well as evaluation criteria (Section M) which will need to address program protection elements. See Attachment D-4 for specific language. (SSE Acq Guidebook, para 3.2, 3.3)

When the Request for Proposal (RFP) is complete the engineering team needs to begin planning for program execution. The engineering team should:

- Update Program level plans/guides (program protection plan, cybersecurity protection plan, Anti-tamper plan, security classification guide, etc.
- Define the organization and insure that the team is aware of their responsibilities.
- The risks developed at the end of the previous phase must be updated.
- Support should be provided to the program management team to gain release of the RFP.
- When the proposals are submitted, they need to be reviewed to ensure that all requirements (SRD & SOW) / deliverables are addressed and evaluated in accordance with the evaluation criteria (Attachment D-4) to support offeror selection and contract award.

Program Execution (through CDR)

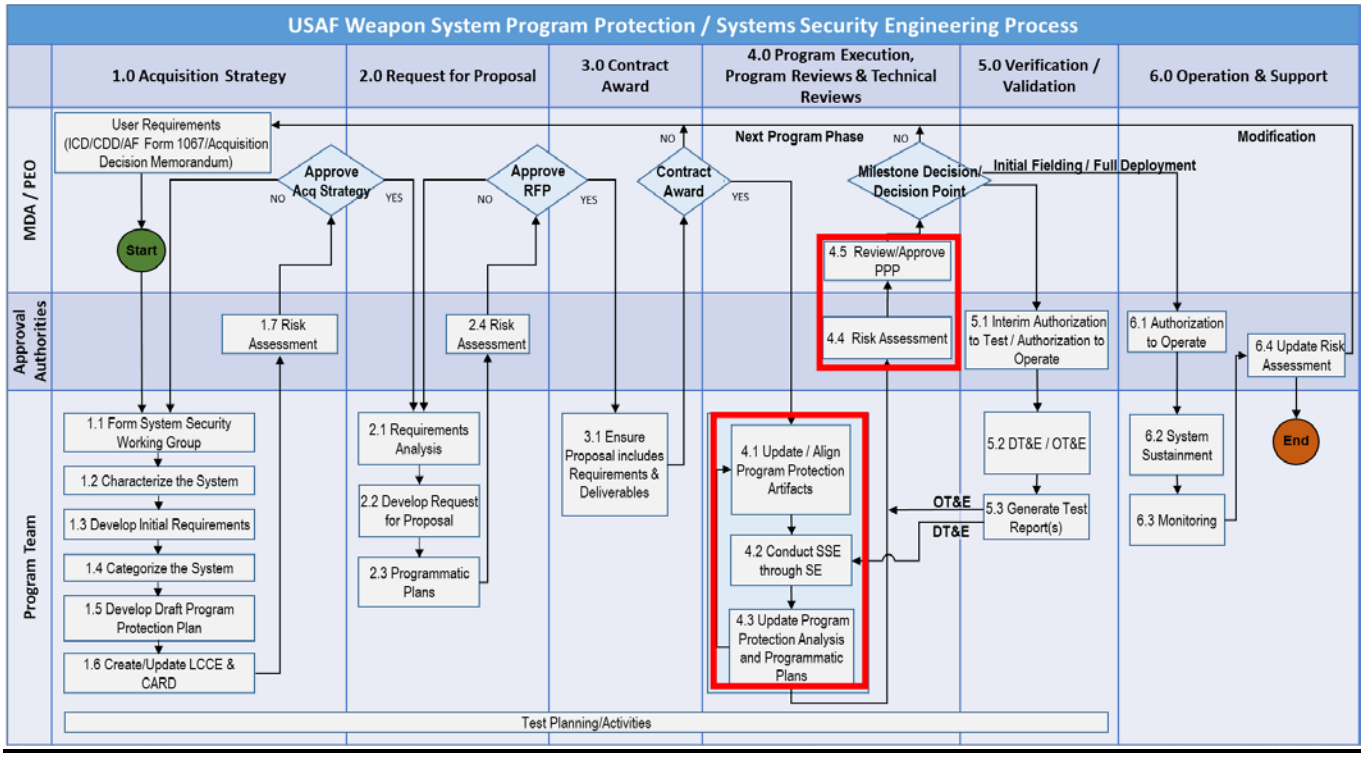


Figure D-14. PP/SSE Process – Contract Award through CDR

During the program execution phase, the system will be designed, built, and lab tested at the subsystem/software level and integrated via laboratory testing. Actions in the Program Execution phase will follow the tasks defined in the SOW (see Attachment D-1). This phase will begin by working with the

contractor selected in the last phase to develop the plans and documentation (CDRLs – see Attachment D-2) captured in the Statement of Work that was put on contract. Working groups need to be established early in the design phase. These include System Safety Working Group, Systems Security Working Group, Test Working Group, and Cockpit Working Group, Cyber Working Group. As the design progresses these groups will support the development effort. Early design focus is on requirements and architecture development, looking at:

- Functional Thread Analysis (FTA) to ensure the hardware selected will support the level of integrity necessary,
- Software development requirements are defined.

Other actions that need to be completed early in this phase include:

- Updates to the program protection plan to identify security elements that must be incorporated in the design to mitigate/eliminate risks to the lowest level.
- Continue to examine the risks identified in earlier phases and develop/refine mitigation plans. All risk mitigations are budgeted.
- Establish a System Safety Working Group and a risk database to capture / identify additional hazards, mitigation plans, and assess risk levels.

System Design Considerations and Practices (SSE Acq Guidebook, para 4.1.2)

The following are overarching system design considerations and practices that should be evaluated as part of the systems engineering process used initial design and architecture definition. These also support CSA requirement 8.4.1.

- Aircraft Systems are not installed without rigorous safety assessments. Any system interconnection effects are integral to the safety assessment process (specific highlights below). The fail-safe design concept is inherent to approved designs. [ASISP Working Group – Final Report August 22, 2016]
- The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e., to ensure that major failure conditions are improbable and that catastrophic failure conditions are extremely improbable.
  - Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures.
  - Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.
  - Isolation of Systems, Components, and Elements so that the failure of one does not cause the failure of another. Isolation is also termed independence.
  - Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.
  - Failure warning or Indication to provide detection and isolation.
  - Flight Crew Procedures for use after failure detection, to enable continued safe flight and landing by specifying crew corrective action.
  - Checkability: the capability to check a component's condition (e.g. start-up BIT, pre-engage or pre-mission IBIT, Maintenance BIT).
  - Designed Failure Effect Limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.

Designed Failure Path to control and direct the effects of a failure in a way that limits its safety impact.
- Margins or Factors of Safety to allow for any undefined or unforeseeable adverse conditions. (e.g., Ultimate load factor of 1.5 MIL-HDBK-516C Section 5, JSSG 2006).

Error-Tolerance that considers adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation [AC 25.13091A dated June 1988]

System Requirements Review / System Functional Review (SRR/SFR) (SSE Acq Guidebook, para 4.1.2, 4.1.3)

The first step in the design process is to understand and decompose the requirements – starting from the SRD, to a System Specification, and down to Critical Item Development Specifications. This decomposition results in the subsystem requirements mapped to each of the 10 Cyber Survivability Attributes (CSA). These recommended subsystem requirements were further assessed and tailored as required. Additional discussion on subsystem requirements is provided in the UAS Modification discussion. See embedded subsystem specification worksheet, which includes tailoring rationale:

Subsystem Requirements

Systems Requirements Review / System Functional Review (SRR/SFR) exit criteria include:

- System Architecture Defined
- System Requirements Document
- SRR/SFR level FTA
- Critical Component / Critical Program Information (CC/CPI) analysis completed
- Anti-Tamper (AT) Plan updated
- Cybersecurity strategy defined
- Supply Chain Risk Management Plan included within the Security Plan
- SSE mapped to program documents (Systems Engineering Plan, Test and Evaluation Plan, Risk Management Plan and Life Cycle Sustainment Plan)
- Contractor Program Protection Implementation Plan delivered and reviewed
- Update Program Security Classification Guide(s)

Preliminary Design Review (PDR) (SSE Acq Guidebook, para 4.1.4)

Further decomposition of the UAS architecture is shown in **Figure D-15**. The colors in the figure designate whether the function is located in the AV segment (Blue), GCS (Green) or spans the two (Gradient).

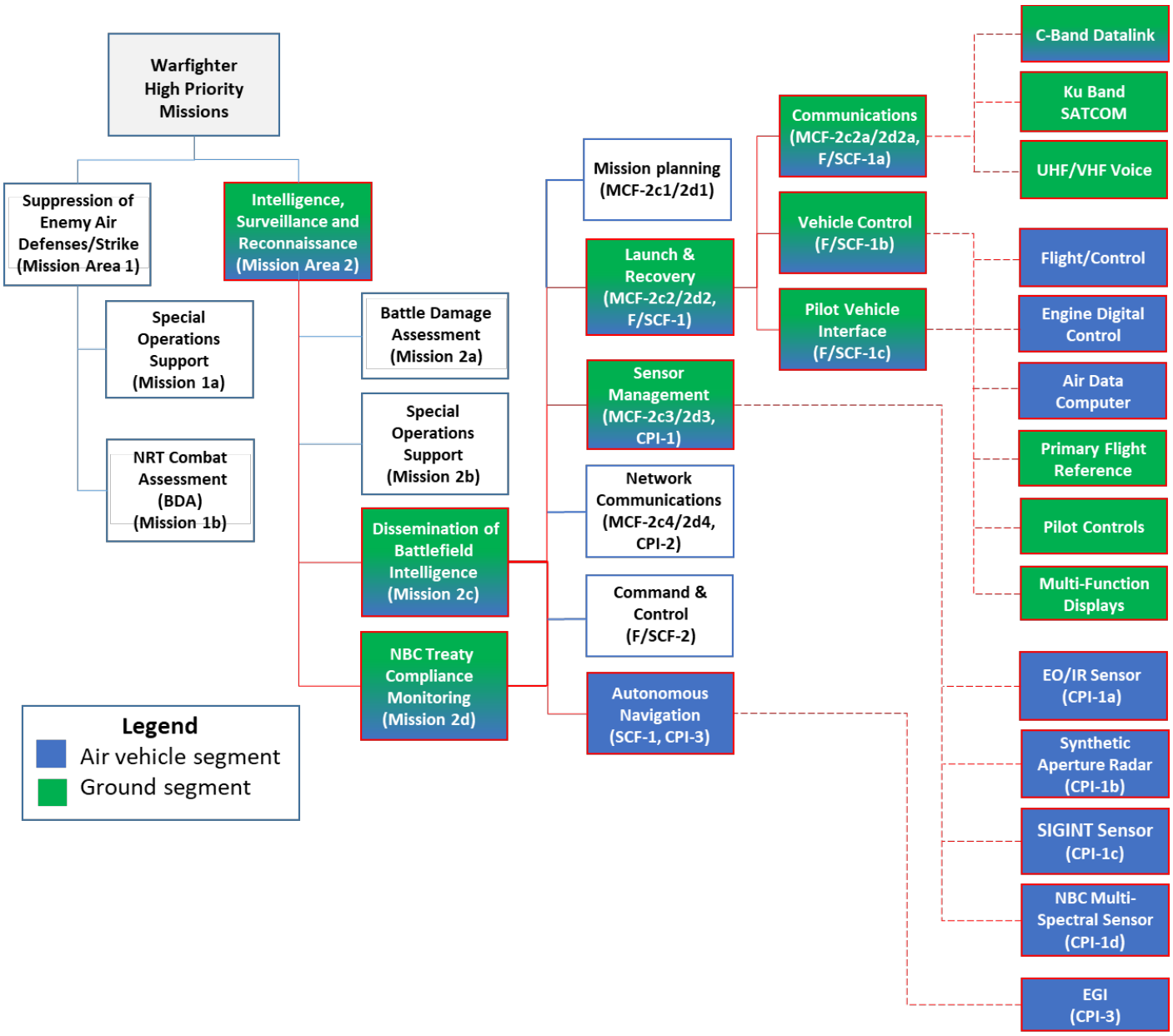


Figure D-15. Updated ISR Functional Thread for Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring

From this point the requirements are decomposed into the components of the system establishing the allocated design. The identified security requirements must be examined at the PDR to ensure that the hardware and software design will protect the system IAW the plans in place. Exit criteria at the PDR include:

- System Architecture baselined
- Allocated requirements approved
- Select subsystem PDR actions and risks are flowed to the Weapon System Review.

- Updated FTA reviewed
- Systems Security Risks and Mitigations reviewed and updated
- Manufacturing sources associated with key CC/CPI identified
- Hardware and Software assurance levels defined for CC/C PI and documented in the design specification and SDP
- Initial Functional Thread Analysis (FTA) completed and critical functions are defined.
- AT plan approved by Anti-Tamper Executive Agent (ATEA) and Program Executive Officer (PEO)
- Cybersecurity Strategy and Plan approved
- Attack path analysis is approved

The FTA is updated to provide supporting components (HW and SW) and the associated system impact for each mission (Dissemination of Battlefield Intelligence **(Table D-5a)** and NBC Treaty Compliance Monitoring **(Table D-5b)**. The attack path analysis results, focusing on the Subsystems containing CC/CPI within the UAS Security Boundary is provided in **Table D-6**. The analysis identifies key interfaces to evaluate for potential vulnerabilities through the program life cycle. The attack path analysis also supports isolating safety critical functions and their vulnerability to attack from non-safety critical functions.

Table D-5a: Updated Functional Thread Analysis Results (Dissemination of Battlefield Intelligence)

Mission	Critical Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I,II,III,IV)
Dissemination of Battlefield Intelligence	Mission Planning (MCF-2c1)	Joint Mission Planning System	I
	Communications (F/SCF-1a; MCF-2c2a)	C Band Data Link (including antenna) and SW	I
		Ku Band SATCOM	II
		UHF/VHF Voice Communications	III
	Vehicle Control (F/SCF-1b)	Flight Control	I
		Propulsion System and SW	I
		Subsystem Controls	I
	Pilot Vehicle Interface (F/SCF-1c)	Primary Flight Reference	I
		Pilot Controls	III
		Displays	I
	Sensors (MCF-2c3; CPI-1a,1b,1c)	EO/IR Sensor - Sensor Head (CPI-1a)	II
		SAR Radar - Transmit / Receive Modules (CPI-1b)	II
		SIGINT System - Mission Data File (MDF) and Digital Receiver (CPI-1c)	II
	Network Communications (MCF-2c4, CPI-2)	Communications Relay - Processor SW (CPI-2)	I
	Command and Control (F/SCF-2)	Ground Control Segment Processor	I
	Autonomous Navigation (SCF-1; CPI-3)	Embedded GPS/INS and Radar Altimeter (including antenna) and SW - Fiber optic gyros and antenna electronics (CPI-3)	I

Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible

Table D-5b: Updated Functional Thread Analysis Results (NBC Treaty Compliance Monitoring)

Mission	Critical Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I,II,III,IV)
NBC Treaty Compliance Monitoring	Mission Planning **(MCF-2d1)**	Joint Mission Planning System	**I**
	Communications **(F/SCF-1; MCF-2d2a)**	C Band Data Link (including antenna) and SW	**I**
		Ku Band SATCOM	**II**
		UHF/VHF Voice Communications	**III**
	Vehicle Control **(F/SCF-1)**	Flight Control	**I**
		Propulsion System and SW	**I**
		Subsystem Controls	**I**
	Pilot Vehicle Interface **(F/SCF-1)**	Primary Flight Reference	**I**
		Pilot Controls	**III**
		Displays	**I**
	Sensors **(MCF-2d3; CPI-1a,1d)**	EO/IR Sensor - Sensor Head **(CPI-1a)**	**II**
		Multi-Spectral Sensor Pod - Sensor Head **(CPI-1d)**	**I**
	Network Communications **(MCF-2d4, CPI-2)**	Communications Relay - Processor SW **(CPI-2)**	**I**
	Command and Control **(F/SCF-2)**	Ground Control Segment Processor	**I**
	Autonomous Navigation **(SCF-1; CPI-3)**	Embedded GPS/INS and Radar Altimeter (including antenna) and SW - Fiber optic gyros and antenna electronics **(CPI-3)**	**I**

Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible

Table D-6: Attack Path Analysis – Critical Subsystems Supporting Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring

	C Band Data Link	UHF/VHF Radio	Ku Band SATCOM	Flight Control Computer & SW	Engine Digital Controller & SW	Air Data Computer & SW	Embedded GPS/INS	EO/IR Seeker	SAR Array	SIGINT Processor SW	Multi-Spectral Sensor Pod	Primary Flight Display & SW	Pilot Controller	Mission Sensor Display & SW	Mission Planning Computer & SW
C Band Data Link					Encrypted Link	Encrypted Link		Encrypted Link	Encrypted Link	Encrypted Link	Encrypted Link	Encrypted Link			Encrypted Link
UHF/VHF Radio			VOIP Encrypted										VOIP Encrypted		
Ku Band SATCOM		VOIP Encrypted											VOIP Encrypted		
Flight Control Computer & SW	Encrypted Link					1553 and Discrete	1553 and Discrete								
Engine Digital Controller & SW	Encrypted Link			1553 and Discrete		1553 and Discrete									
Air Data Computer & SW				1553 and Discrete	1553 and Discrete										
Embedded GPS/INS	Encrypted Link			1553 and Discrete				1553	1553	1553	1553	Encrypted Link			
EO/IR Seeker	Encrypted Link						1553						Encrypted Link	Encrypted Link	
SAR Array	Encrypted Link						1553						Encrypted Link	Encrypted Link	
SIGINT Processor SW	Encrypted Link						1553						Encrypted Link	Encrypted Link	
Multi-Spectral Sensor Pod	Encrypted Link						1553								
Primary Flight Display & SW	Encrypted Link						Encrypted Link						Ethernet		
Pilot Controller	Encrypted Link	VOIP Encrypted	VOIP Encrypted									Ethernet		Ethernet	Encrypted Ethernet
Mission Sensor Display & SW	Encrypted Link												Ethernet		
Mission Planning Computer & SW													Encrypted Ethernet	Encrypted Ethernet	

The preliminary MIL-STD-1553, ethernet, and discrete interfaces are documented in configuration management controlled Interface Control Documents (ICD).

As part of exit criteria for PDR, an updated risk assessment was conducted based on the cybersecurity requirements identified and an understanding of preliminary subsystem design and decomposition of UAS architecture. This is shown in **Figure D-16**.

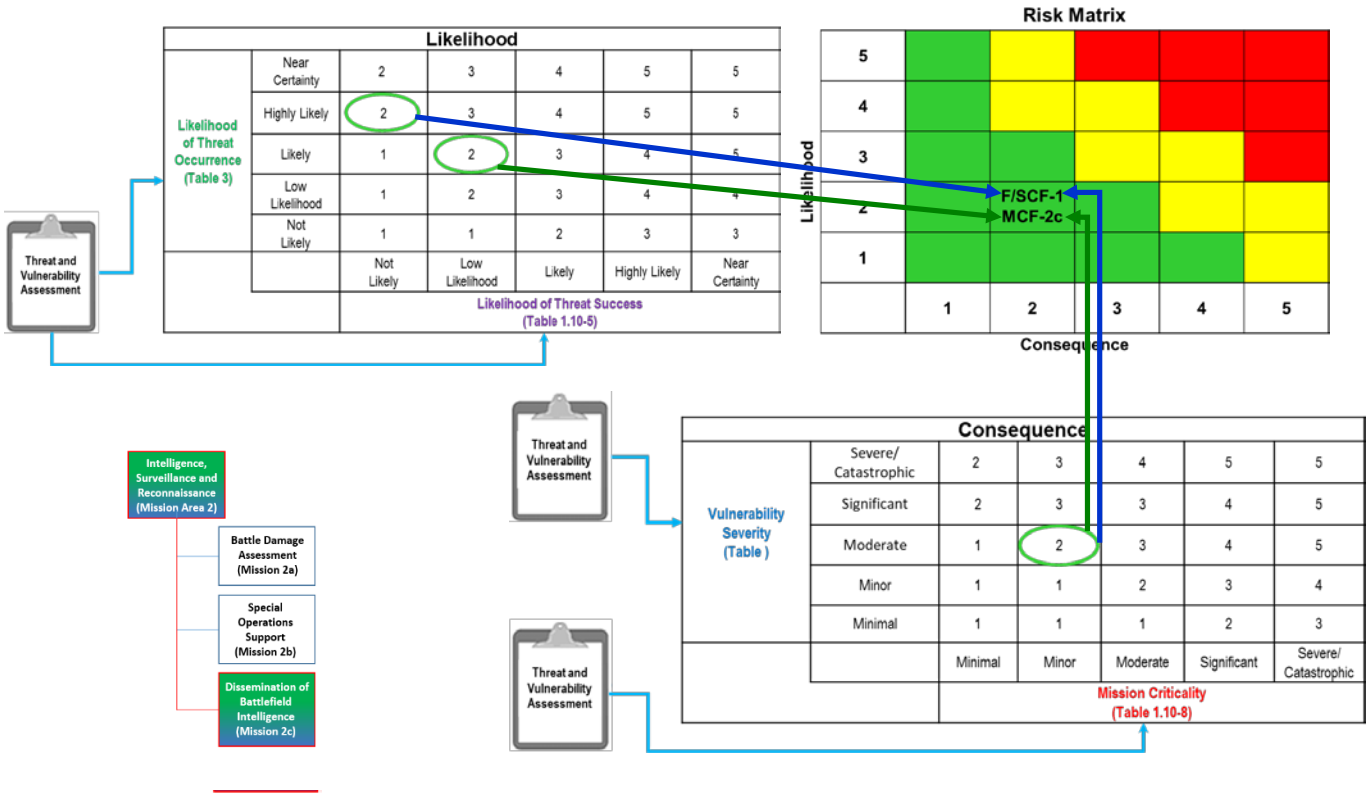


Figure D-16. Mitigated Risk for MCF-2c and F/SCF-1

Critical Design Review (CDR) (SSE Acq Guidebook, para 4.1.5)

The detailed HW and SW design completed. Exit criteria at the CDR include:

- Select subsystem CDR actions and risks are flowed to the Weapon System Review.
- TEMPEST Control Plan reviewed
- Modeling and Simulation accreditation validation / verification plan approved
- Hardware and Software design documentation baselined
- AT requirements updated
- Updated FTA reviewed
- CC/CPI updated
- Final ICDs are approved
- Cybersecurity risks, mitigations, and attack path analysis updated, if required.
- SSE risks updated and mitigations updated
- SSE test plans and procedures completed and reviewed, including SIL and FMET.

Part 2: Aircraft System Modification

This next section explores a separate scenario for a program that is a modification, or upgrade, to an existing aircraft system. This scope of this scenario is to ensure PP/SSE in the design of the modification, while also integrating these into the existing Program Protection Plan and SSE efforts of the whole weapon system.

Warfighter Statement of Need: (SSE Acq Guidebook, para 1.1.1)
Headquarters Air Combat Command (ACC) has defined mission deficiencies coming out of Development and Operational Test & Evaluation (DT&E/OT&E) as well as mission operations that require improvements in the areas below. The modification contract is issued sole source to the existing prime. As such, there was no competitive Request for Proposal Issued by the USG Program Office.

- Air Vehicle
  - RF and IR sensor software improvements
  - Mission data transmission improvements
  - Enhanced Global Positioning System (GPS) security (SASSM + M-Code)
- Ground Control Segment
  - Post mission processing sensor fusion software improvements
  - Processor Tech Refresh (due to DMS/MS)

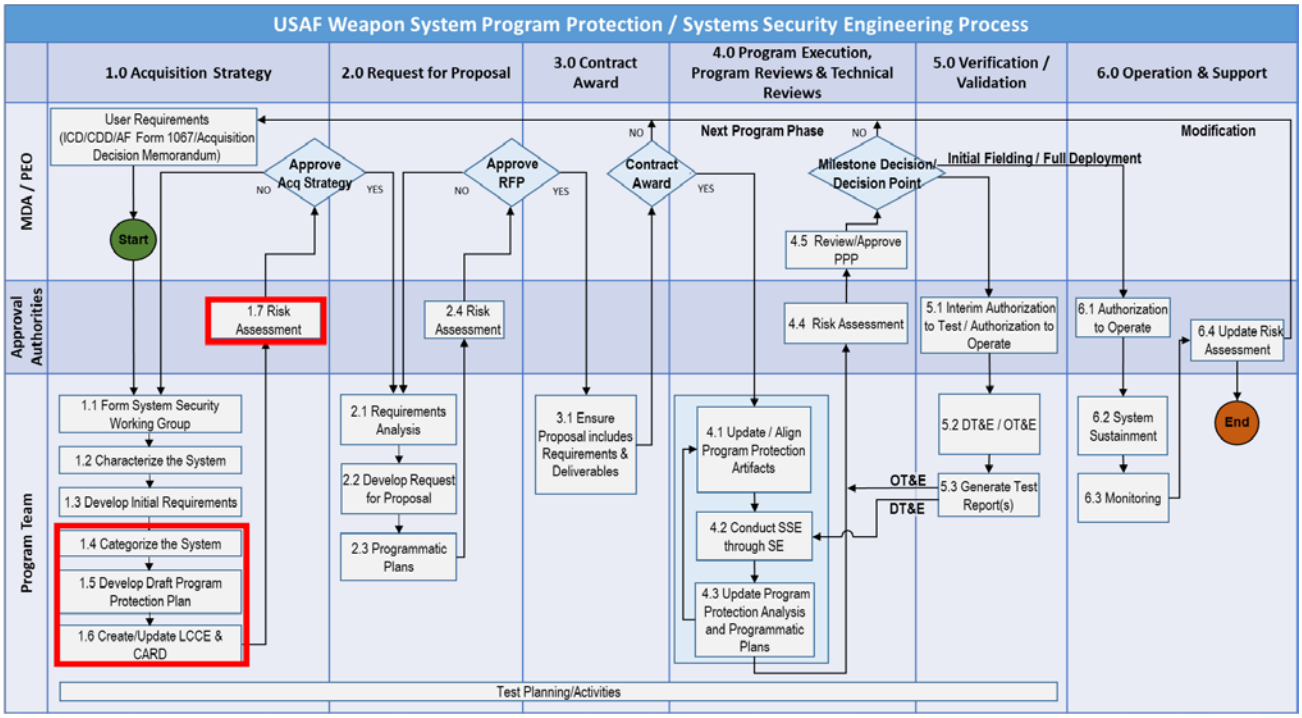


Figure D-17. PP/SSE Process Flow – Modification Requirements Development

A residual cybersecurity risk defined during OT&E is the probability of spoofing the existing platform GPS. The mitigated risk at the end of OT&E and unmitigated risk for the modification is shown in **Figure D-18**. At Preliminary Design Review (PDR) for the program, the only navigation capability to provide precision navigation was an off-the-shelf Embedded GPS / INS (EGI) subsystem sufficient to provide long term

navigation and precision position and velocity sufficient to support High Resolution imagery collection and the required precision weapon target location error (TLE). The residual cybersecurity risks were assessed as a Moderate Consequence with a Likelihood value of "2".

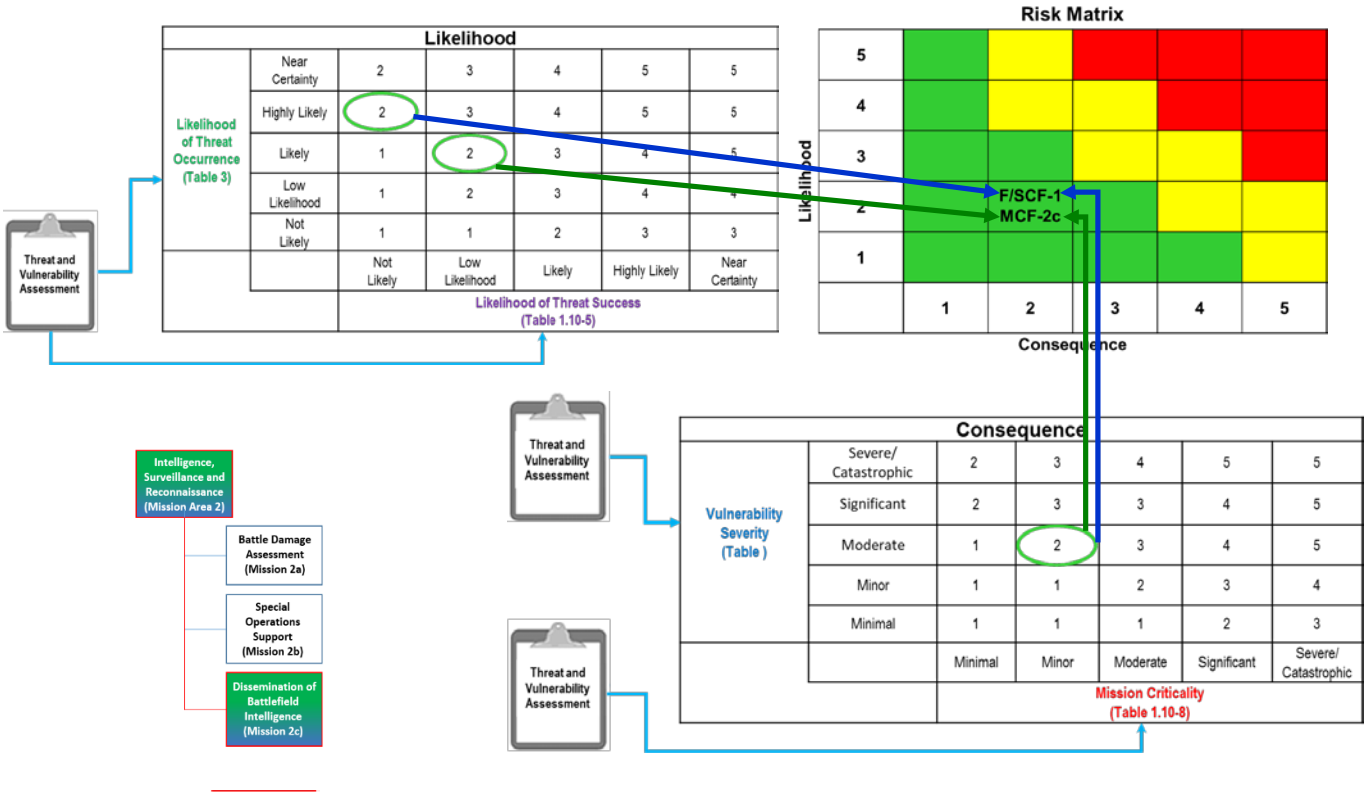


Figure D-18. Modification Initial Unmitigated Risk Assessment - Modification

Weapon System High Priority Missions

There are no changes to existing mission areas and high priority missions **(see Figure D-3)**:

1. Intelligence, Surveillance, and Reconnaissance (ISR) operations

   *a. Dissemination of Battlefield Intelligence**
   *b. Special Operations Support**
   *c. Battle Damage Assessment (BDA)**
   d. Blockade and Quarantine Enforcement
   e. United Nations (UN) Treaty Monitoring
   f. Humanitarian Aid Support
   g. Border Control and Drug Enforcement
   h. *NBC Treaty Compliance Monitoring**

2. Suppression of Enemy Air Defenses (SEAD) / Near-Real-Time (NRT) Strike

   *c. Special Operations Support**
   *d. NRT Combat Assessment**

   **These missions have been identified as highest priority by Warfighter*

Functional Thread Analysis (FTA)

The starting point for the modification is the baselined FTA at the end of the EMD phase. Changes in boundaries due to the modification or the mission, changes in functionality (hardware and software), and identified residual cybersecurity risks from EMD form the starting point for the FTA for this modification.

System-Level Description & Environmental Considerations

- The existing EGI is replaced with a Resilient Selective Availability Anti-Spoofing Module (SASSM) and a M-Code capability to utilize enhanced resilient GPS signals. The Resilient EGI (R-EGI) is deemed flight safety critical. Also required, is a modification to the GPS antenna receiver electronics unit to support M-Code reception.
- The Ground Station post mission processor requires Central Processing Unit (CPU) card replacement. The existing processor backplane is an open VPX design. The processor boards are form-fit replaceable.
- Ground Station post processing of mission sensor data has limitations in fusion engine software design. A better understanding of AV RF and IR sensor performance (accuracy, mode timelines) requires enhancements in sensor integration.
- Corresponding optimization of AV sensor mode software and interleave logic as well as sensor cueing improvements is required.
- Sensor and post mission processing improvements require corresponding changes in datalink sensor information content (no required changes in datalink hardware). Interface Control documentation between sensors and AV mission C-Band Datalink is updated. Likewise, Interface Control documentation between GCS C-Band Datalink and GCS processing are updated.
- No changes are required to datalink encryption.
- A Modification Airworthiness Certification Criteria (MACC) is required, since primary navigation safety critical functional threads are impacted.
- Positioning, Navigation, and Timing (PNT) certification is required.
- Internal Connectivity - For the UAS, internal connectivity consists of analog and discrete I/O, bi-directional serial data busses (e.g., MIL-STD-1553, ARINC 429, RS-232, Ethernet) and some parallel data bus communications (e.g. PCI) as well as NIPRNet, SIPRNet.
- External Connectivity:
  - External AV Segment connectivity requirements includes commercial SATCOM, INMARSAT, Link-16, GPS, Military SATCOM, VHF/UHF, SAP/JWICS, Common Data Link (CDL), etc.
  - External GCS Segment connectivity adds NIPRNet, SIPRNet, SAP/JWICS, Cross-domain data transfer to/from those networks, and 802.11 Wireless

Assumptions regarding “untrusted” interactions:

- Personnel interactions (operators, maintainers, developers) are considered trusted because of physical security provisions assumed to be in place. That doesn’t preclude unintentional security vulnerabilities associated with personal electronic devices (PED) with access to the internet as an example.
- GPS, SATCOM, ILS, ATC and other sources of NAS data are assumed trusted; communication links are considered vulnerabilities.
- Defense Intelligence Agency Threat Assessment Center (DIA TAC) - DoD has designated the Defense Intelligence Agency (DIA) to be the DoD enterprise focal point for threat assessments needed by the DoD acquisition community to assess supplier risks.

- Safety critical developmental processes are utilized to provide reduction in vulnerability risks due to untrusted interactions; for example, levels of rigor assignments to safety critical software. Detailed Safety Critical Functional Thread Analyses (SCFTA) have been updated to support UAS modifications. Levels of Rigor are maintained through this modification.
- Anti-tamper implementations to protect Critical Program Information (CPI) and Critical Components (CC) are leveraged to bake-in cybersecurity resiliency.

Modified UAS architecture elements are indicated in **Figure D-19**.

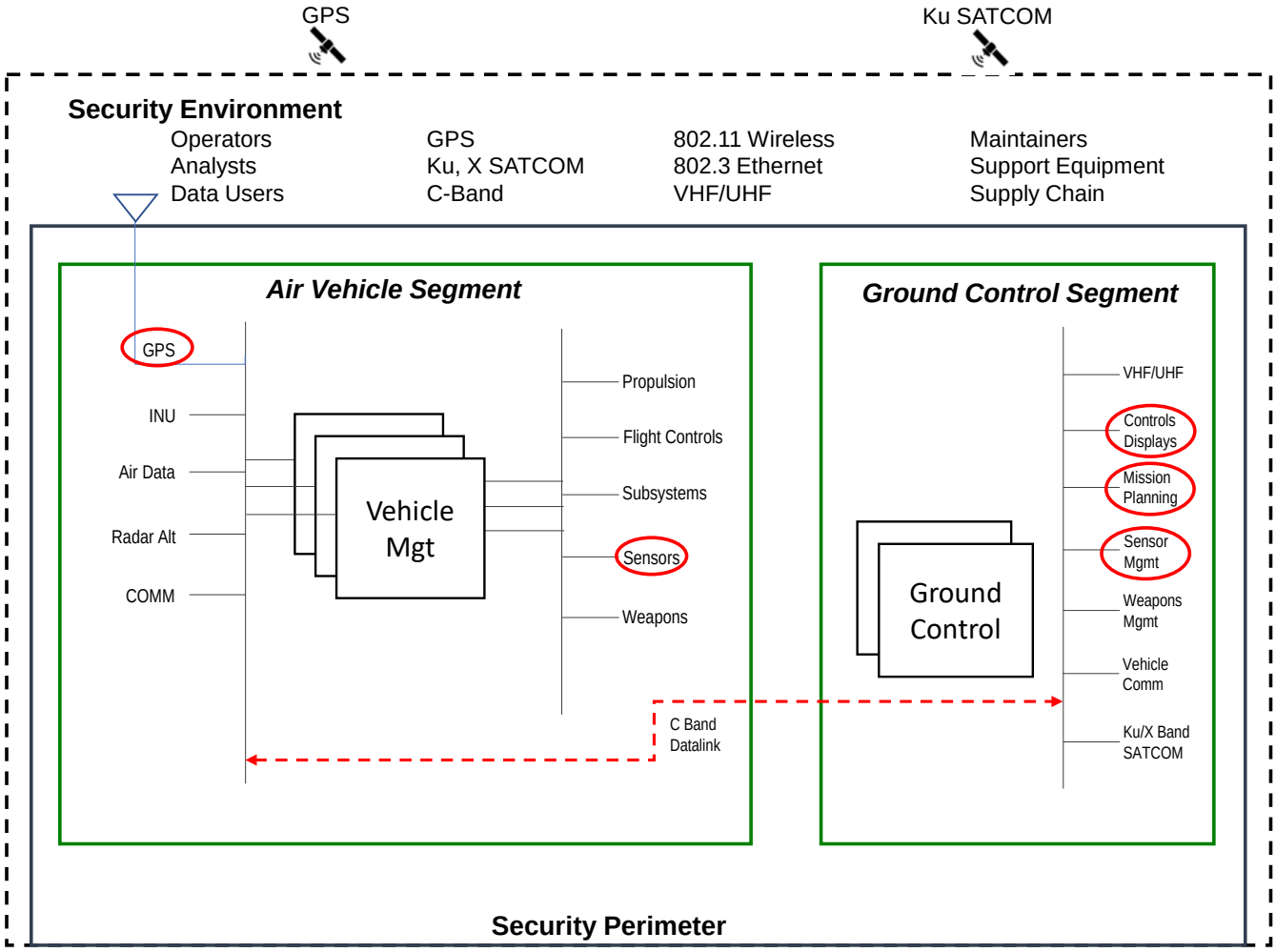


Figure D-19. UAS Modification Security Boundaries

Initial CC/CPI Identification/ Analysis (SSE Acq Guidebook, para 1.1.2)

There are no new CC/CPI changes from the baseline program. CC/CPI are identified in Autonomous Navigation, Sensor Management, Network Communication, Hi Res SAR, and several Sensor Fusion Post-Processing subsystems. The new Resilient EGI GPS subsystem is part of Autonomous Navigation functionality.

Cyber Survivability Endorsement & Cyber Survivability Attributes (SSE Acq Guidebook, para 1.1.1)

As shown in **Table D-1** for the baseline, this modification also assumes a Cyber Survivability Risk Category of 3.

The Cyber Survivability Attributes to be applied to the system's high priority missions were identified early in the baseline MAE UAS program and revalidated for the Precision Navigation upgrade modification. The tailored CSAs provided in **Table D-2** above are unchanged for this modification.

Table D-2: User Tailored Cyber Survivability Attributes (Repeated from above)

CSA	Pillar	Cyber Survivability Attribute (CSA) **Need to be tailored**	Dissemination of Battlefield Information		NBC Treaty Compliance Monitoring	
			Applicable to the AV Segment (Yes/No)	Applicable the GCS (Yes/No)	Applicable to the AV Segment (Yes/No)	Applicable to the GCS (Yes/No)
CSA 01	Prevent	The system ensures that only identified, authorized and approved persons and non-person entities are allowed access or interconnection to the system.	**No** Physical security controls (guards, gates, accesses) in place for AV prevent the need for further dedicated controls for CSA 01.	**Yes**	**No** Physical security controls (guards, gates, accesses) in place for AV prevent the need for further dedicated controls for CSA 01.	**Yes**
CSA 02	Prevent	Wireless and wired signaling and communications should not compromise OPSEC.	**Yes**	**Yes**	**Yes**	**Yes**
CSA 03	Prevent	All intelligence dissemination transmissions and communications shall be maintained at the appropriate security level (e.g. secret, top secret, TS-SCI).	**Yes**	**Yes**	**Yes**	**Yes**
CSA 04	Prevent	The system defends against adversary attempts to exploit information resident in the system. The system counters attempted malicious data injection, other corruption, or denial of service activities. The system also protects information at rest, against corruption, exploitation or exfiltration.	**Yes**	**Yes**	**Yes**	**Yes**

CSA	Pillar	Cyber Survivability Attribute (CSA) **Need to be tailored**	Dissemination of Battlefield Information		NBC Treaty Compliance Monitoring	
			Applicable to the AV Segment (Yes/No)	Applicable the GCS (Yes/No)	Applicable to the AV Segment (Yes/No)	Applicable to the GCS (Yes/No)
CSA 05	Prevent	The system's safety and mission critical functions are isolated from less critical functions. The system preserves minimum essential performance for mission critical and supporting platform functions.	**Yes**	**Yes**	**Yes**	**Yes**
CSA 06	Prevent	Minimize and Harden Cyber Attack Surfaces	**Yes**	**Yes**	**Yes**	**Yes**
CSA 07	Mitigate	The system monitors for cyber anomalies (e.g. leaks, intrusions, and attack effects) in critical functions, components, and communications. The 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. The system logs all cyber anomalies in non-volatile memory.	**Yes**	**Yes**	**Yes** However, mission does not drive additional mitigations to cyber vulnerabilities beyond the mitigations in place for other priority missions.	**Yes** However, mission does not drive additional mitigations to cyber vulnerabilities beyond the mitigations in place for other priority missions.
CSA 08	Mitigate	No single failure results in the inability to complete the mission(s).	**Yes**	**Yes**	**No** NBC Multi-Spectral Sensor Pod does not incorporate redundancy. If sensor fails, mission is terminated.	**Yes**
CSA 09	Recover	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.	**Yes**	**Yes**	**No** NBC Multi-Spectral Sensor Pod does not incorporate redundancy. If sensor fails, mission is terminated.	**No** Loss of Ground Station real time monitoring backed up by sensor pod data recorder.
CSA 10	Prevent Mitigate Recover	Actively Manage System's Configuration to Counter Vulnerabilities at rest, prior to and during all mission phases.	**Yes**	**Yes**	**Yes**	**Yes**

Initial Functional Thread Analysis (SSE Acq Guidebook, para 1.1.2)

The results of the analysis for the baseline program remain valid. Mission critical functions shown in Tables 5a and 5b for the Dissemination of Battlefield Information and NBC Treaty Compliance Monitoring are unchanged.

Mission decomposition to functional threads as shown in **Figure D-20** are unchanged, with the exception of the replacement of the EGI with the R-EGI.

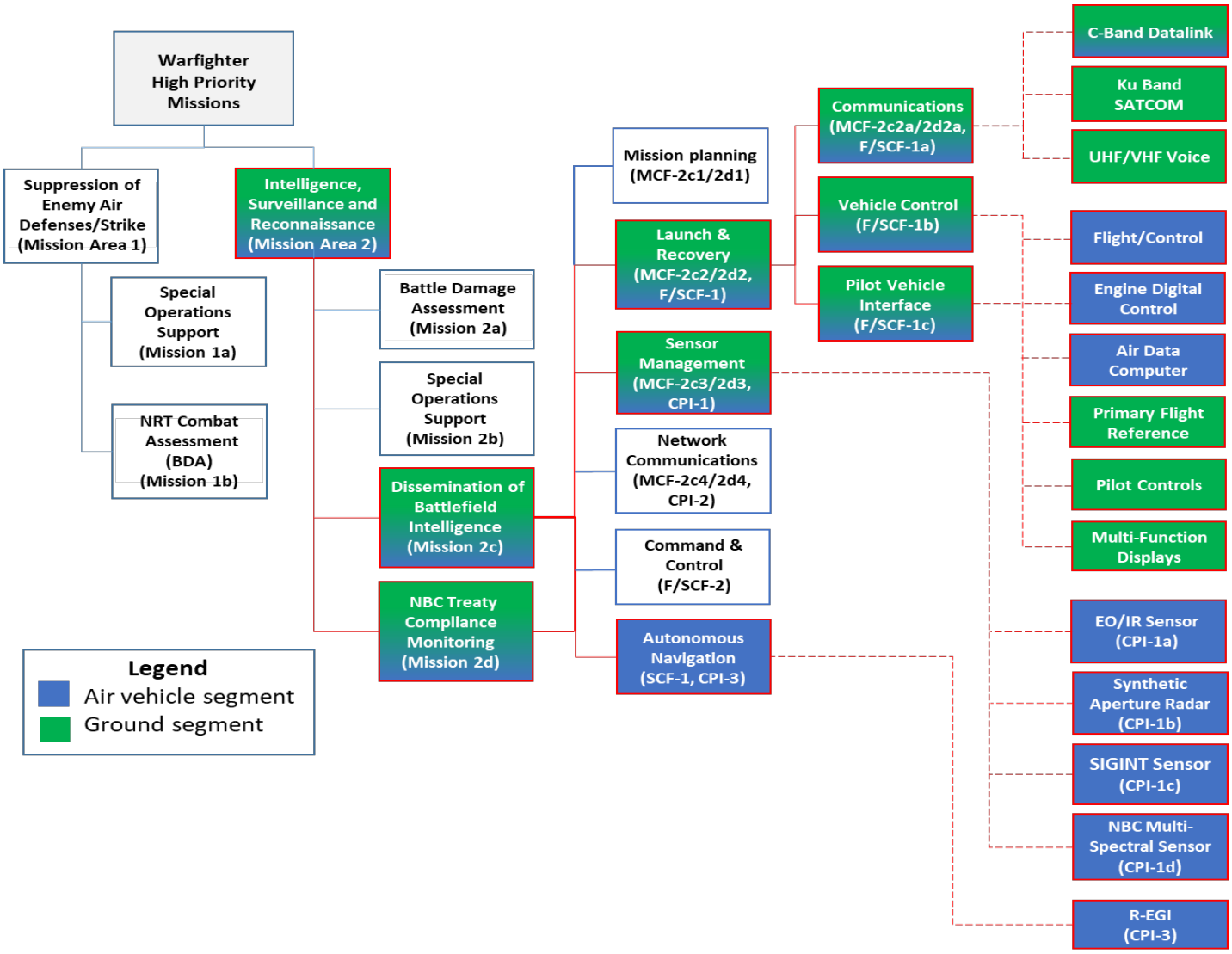


Figure D-20. Updated ISR Functional Thread for Dissemination of Battlefield Intelligence and NBC Treaty Compliance Monitoring

Identify Initial Vulnerability & Threats (SSE Acq Guidebook, para 1.10)

The Validated On-Line Lifecycle Threat (VOLT) assessment concludes after review of threats that vulnerabilities and threats for the modification are unchanged.

Develop Initial Requirements and Analysis (SSE Acq Guidebook, para 2.2)

At the System Level, the Systems Security Engineering (SSE) requirements for the modification are unchanged. The collective verification documentation of these requirements provides the starting point for the verification of these requirements for this modification program.

The SSE system and subsystem level requirements for the MAE UAS Modification are provided in **Table D-7** below. Subsystem requirements are focused on the specific elements of this modification. A detailed SSE requirements worksheet is attached below. Rationale for tailoring / deletion of recommended requirements is included.

UAS Modification Requirements

Table D-7: SSE Requirements

Requirement	System Specification Requirements (Tailored for UAS Modification)	Air Vehicle Specification	Ground Control Segment Specification
Prevent		**CSA 01 - Control Access**	
1.1a	The system shall ensure that the Ground Control Segment is accessed only by authenticated persons and authenticated external interconnections to the system or internal interconnections with sub-elements within the security boundary.		1.1.1a 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.
			1.1.1b The system shall provide the capability to display approved DOD login banner with the following attributes. 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

			4. Use of the information system indicates consent to monitoring and recording; 5. Classification banner
1.2	The system shall enforce least-privilege access for authenticated persons and non-person entities necessary to accomplish assigned tasks.		1.2.3 The system shall prevent unauthorized privilege escalation.
1.2			1.2.4 The system shall require privileged access to complete vulnerability scanning, system logs, and system updates.
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 IAW MIL-STD-464, paragraphs 5.13 and 5.14.	2.1.1 The Air Vehicle shall protect system components, associated data communications, and networks in accordance with (i) electromagnetic signals emanations IAW MIL-STD-464, paragraphs 5.13 and 5.14.	The system shall protect against adversary detection and exploitation of information leakage due to electromagnetic emanations IAW MIL-STD-464, paragraph 5.14.
2.2	The system shall minimize wired and wireless signals to generate and upload mission plans in accordance with Emissions Control (EMCON), using AFGSCI 10-707 as guidance.	2.2.2 The Air Vehicle shall provide the capability to reduce the transmission power of radio frequencies to prevent signal usability outside of the intended operational area.	2.2.2 The Ground Control Segment shall provide the capability to reduce the transmission power of radio frequencies to prevent signal usability outside of the intended operational area.
Prevent		**CSA 03 - Secure Transmissions and Communications**	
3.1	The system shall encrypt all data link transmissions and communications of data in transit external to the Air vehicle and Ground Control Segments at the appropriate classification levels.	3.1.1 The Air Vehicle shall encrypt both unclassified and classified crypto keys at startup and at rest.	3.1.1 The Ground Control Segment shall encrypt both unclassified and classified crypto keys at startup and at rest.
		3.1.4 The Air Vehicle shall implement cryptographic keys per NSA/FIPS standards.	3.1.4 The Ground Control Segment shall implement cryptographic keys per NSA/FIPS standards.
Prevent		**CSA 04 - Protect System's Information from Exploitation**	
4.1	The system shall ensure information integrity and system performance	4.1.2 The Air Vehicle shall provide the capability to:	4.1.2 The Ground Control Segment shall provide the capability to:

	sufficient to complete priority missions after any single cyber event.	a) Install verified and authenticated software and firmware. b) Reject the installation of non-verified and non-authenticated software and firmware.	a) Install verified and authenticated software and firmware. b) Reject the installation of non-verified and non-authenticated software and firmware.
		4.1.4 The Air Vehicle shall validate information input and output to ensure the information is consistent with the expected content.	4.1.4 The Ground Control Segment shall validate information input and output to ensure the information is consistent with the expected content.
		4.1.7 The Air Vehicle shall implement a secure boot and verify the integrity of the boot process.	4.1.7 The Ground Control Segment shall implement a secure boot and verify the integrity of the boot process.
		4.1.18 The Air Vehicle shall implement security safeguards to protect its memory from unauthorized code execution.	4.1.18 The Ground Control Segment shall implement security safeguards to protect its memory from unauthorized code execution.
4.3	The system functions containing critical program information (CPI) shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.	4.3.2The Air Vehicle shall employ tamper-evident technologies to deter, prevent, detect, and/or react to attempts to modify CC/CPI.	4.3.2 The Ground Control Segment shall employ tamper-evident technologies to deter, prevent, detect, and/or react to attempts to modify CC/CPI.
		4.3.4 The Air Vehicle shall include the capability to impose programmable hard and / or soft penalties on specified components (reduce system capabilities, force system reset, erase crypto keys).	4.3.4 The Ground Control Segment shall include the capability to impose programmable hard and / or soft penalties on specified components (reduce system capabilities, force system reset, erase crypto keys).
4.4	The system shall implement sanitization processes to protect CPI in all phases of mission execution.	4.4.1 The Air Vehicle shall employ a sanitization function that enables erasing sensitive/classified data to prevent disclosure.	4.4.1 The Ground Control Segment shall employ a sanitization function that enables erasing sensitive/classified data to prevent disclosure.
Prevent		**CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels**	
5.1	The system shall isolate mission critical and safety critical CPI functionality from less critical functions.	5.1.1 The Air Vehicle shall isolate mission critical and safety critical CPI functionality from less critical functions.	5.1.1 The Ground Control Segment shall isolate mission critical and safety critical CPI functionality from less critical functions.

Prevent		CSA 06 – Minimize and Harden Attack Surfaces	
6.1	The system shall configure external interfaces to perform safety critical and mission critical functions.	6.1.3 The Air Vehicle shall provide the capability to enable only ports, protocols and services that are required for mission and safety critical functions.	6.1.3 The Ground Control Segment shall provide the capability to enable only ports, protocols and services that are required for mission and safety critical functions.
		6.1.8 The Air Vehicle shall route all remote access through managed network access control points.	6.1.8 The Ground Control Segment shall route all remote access through managed network access control points.
6.2	The system shall ensure interfaces are hardened, while supporting safety/mission critical functions.	6.2.1 The Air Vehicle shall use secure operating systems and trusted hardware and software.	6.2.1 The Ground Control Segment shall use secure operating systems and trusted hardware and software.
		6.2.2 The Air Vehicle shall implement: a) a managed interface for each external connection (interfaces that require specific rules such as encryption and routing. b) Enforce prevention of unauthorized exfiltration of information c) Restrict communications to only what is required to operate.	6.2.2The Ground Control Segment shall implement: a) a managed interface for each external connection (interfaces that require specific rules such as encryption, routing, and/or firewalls). b) enforce the defined traffic flow policy c) restrict the use of information inputs to only approved, trusted sources and/or formats (e.g. whitelisting for information inputs) d) Enforce strict tunneling for remote access to prevent simultaneous system communication with other networks (split tunneling). e) Enforce prevention of unauthorized exfiltration of information f) Enforce security requirements for Intrusion Detection System (IDS), Intrusion Protection System (IPS), Firewall and Collision Detection System (CDS) g) Restrict communications to only what is required to operate.
Mitigate		**CSA 07 – Baseline & Monitor Systems and Detect Anomalies**	
7.1	The system shall monitor operational parameters, boundaries, and configuration controls.	7.1.1 The Air Vehicle shall monitor operational parameters for anomalies, including but not limited to: a) Timing b) Latency	7.1.1 The Ground Control Segment shall monitor operational parameters for anomalies, including but not limited to: a) Timing b) Latency

		c) Memory allocation (software size, memory storage, etc.) d) CPU allocation e) Unauthorized changes to hardware, software, and firmware f) encryption status g) communications that violate the protocol h) improper formatting of messages i) Out or range or invalid values j) data that is not reasonable in the current circumstances k) built in test	c) Memory allocation (software size, memory storage, etc.) d) CPU allocation e) Unauthorized changes to hardware, software, and firmware f) encryption status g) communications that violate the protocol h) improper formatting of messages i) Out or range or invalid values j) data that is not reasonable in the current circumstances k) built in test l. virus and malware scans
			7.1.6 The Ground Control Segment shall continuously monitor inbound and outbound traffic for unauthorized actions and intrusion detection.
7.2	The system shall analyze performance through a baseline comparison to detect anomalies and attacks.	7.2.1 The Air Vehicle shall analyze performance through a baseline comparison to detect anomalies and attacks	7.2.1 The Ground Control Segment shall employ a detection systems to detect attack attempts and potential compromises/breaches to the system.
7.3	The system shall generate and store mission logs.	7.3.5 The Air Vehicle shall log the occurrence of system resets, anomalies, and system accesses.	7.3.5 The Ground Control Segment shall log the occurrence of system resets, anomalies, and system accesses.
Mitigate	**CSA 08 - Manage System Performance if Degraded by Cyber Events**		
8.1	The system shall alert users of detected anomalies and attacks.	8.1.1 The Air Vehicle shall alert the operator of detected anomalies and attacks without revealing potentially exploitable data.	8.1.1 The Ground Control Segment shall alert the operator(s) of detected anomalies and attacks without revealing potentially exploitable data.

8.3	The system shall maintain mission critical functions in a cyber contested operational environment during/after observed anomaly(ies).	8.3.5 The Air Vehicle shall provide the capability for operators to define sets or sequences of responses, and to invoke a given response set or sequence, to ensure continuity of mission critical functions.	8.3.5 The Ground Control Segment shall provide the capability for operators to define sets or sequences of responses, and to invoke a given response set or sequence, to ensure continuity of mission critical functions.
8.4	The system shall maintain safety and mission critical functions in a cyber-contested operational environment during/after observed anomalies	8.4.1 The Air Vehicle shall maintain safety critical functions in a cyber contested operational environment during/after observed anomalies.	8.4.1 The Ground Control Segment shall maintain safety critical functions in a cyber contested operational environment during/after observed anomalies.
8.5	No single cyber related failure shall result in the inability to complete the mission.	8.5.1 The Air Vehicle shall continue to execute the mission in the event of a single cyber-related failure.	8.5.1 The Ground Control Segment shall continue to execute the mission in the event of a single cyber-related failure.
Recover	**CSA 09 - Recover System Capabilities**		
9.1	The system shall provide the capability to recover to a known operating state in near real time following an anomaly.	9.1.1 The Air Vehicle shall provide the capability to recover to a known safe operating state in near real time following an anomaly.	9.1.1 The Ground Control Segment shall provide the capability to recover to a known operating state in near real time following an anomaly.
		9.1.4 The Air Vehicle shall provide the capability to retrieve and restore system operating information from configuration-controlled and integrity-protected memory.	9.1.4 The Air Vehicle shall provide the capability to retrieve and restore system operating information from configuration-controlled and integrity-protected memory.
P/M/R	**CSA 10 - Actively Manage System Configurations to Counter Vulnerabilities at Tactically Relevant Speeds**		
10.1	The system scans shall have the capability to be updated to ensure appropriate, applicable requirements are captured (e.g., STIGS, SRG, Benchmarks, Configuration, etc.) for: (a) Hardware, (b) Software, and (c) Firmware	10.1.1 The Air Vehicle shall have the capability to be updated to ensure appropriate, applicable requirements are captured (e.g., STIGS, SRG, Benchmarks, Configuration, etc.) for: (a) Hardware (b) Software (c) Firmware	10.1.1 The Ground Control Segment shall have the capability to be updated to ensure appropriate, applicable requirements are captured (e.g., STIGS, SRG, Benchmarks, Configuration, etc.) for: (a) Hardware (b) Software (c) Firmware

Examples of subsystem requirements are as follows:

CSA 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.

- This requirement is deleted as it is covered by requirement CSA 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.
- This is believed sufficient and appropriate for the UAS weapon system, given implemented physical security controls.

CSA 6.1.9: The system shall provide the capability to disable all non-mission critical remote access.

- This requirement is assessed not applicable to the UAS weapon system as all functionality is considered either mission or safety critical and as such, disabling this functionality creates a potential operational safety or mission execution risk.

Requirements Analysis (SSE Acq Guidebook, para 2.2)

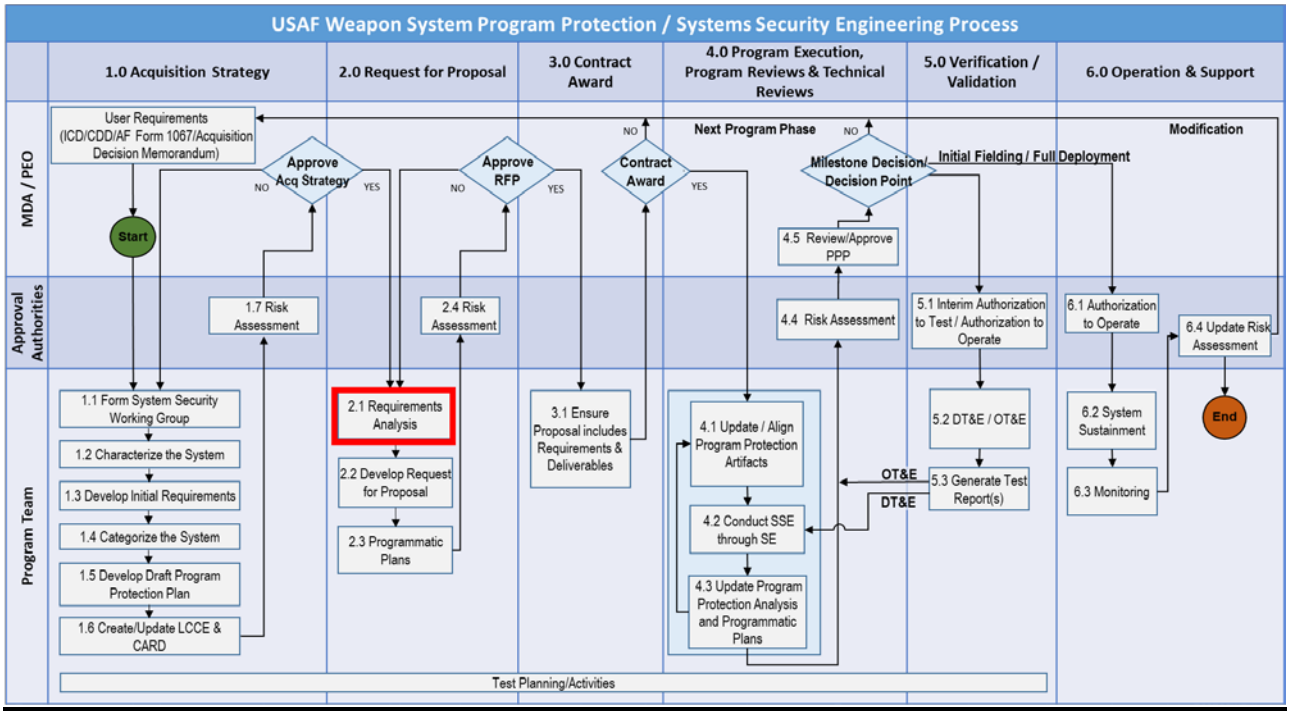


Figure D-21. PP/SSE Process – Requirements Analysis

Requirements analyses are conducted to ensure the correct and relevant requirements are selected, including tailoring, for the UAS modification.

- Since the AV segment is unmanned, requirements 1.1 and 1.2 only apply to the GCS. That might be overstating the case since the AV Segment requires scheduled and unscheduled maintenance and periodic HW/SW updates to on-board systems. The thought is the aircraft would be protected by guards, gates, and guns and therefore not appropriate for the SRD. The GCS would certainly

employ authentication and least privilege access more appropriate for SOW (see Attachment D-1) and Security Plan (see CDRLS in Attachment D-2). **(revalidate baseline including modification)**

- All safety/mission critical hardware elements are qualified to the Electromagnetic Environmental Effects (EEE) requirements in MIL-STD-464, including Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST), Emissions Control (EMCON) (requirement 2.1), Hazards of Electromagnetic Radiation to ordinance (HERO), to Fuel (HERF) and to Personnel (HERP). This is an area where the threat and attack path must be identified to determine if standard design practice is deficient. **(revalidate baseline including modification)**
- For MCF-2c, wireless connections can be controlled via EMCON procedures in the mission plan and encrypted data links. For F/SCF-1, wireless connections are limited to encrypted C-band and UHF/VHF radio Communications. The radios are functionally isolated from the Launch and Recovery function thread. (requirements 2.2 and 3.1) **(revalidate baseline)**
- MCF-2c, F/SCF-1, and F/SCF-2 shall embody the design best practices systems identified in JSSG2005, JSSG 2008, Mil-HDBK-516C, and FAA AC 25.1309-1A **(revalidate baseline including modification)**:
    - Requirement 4.1 - Information integrity and performance is ensured by the HW/SW development processes applied to safety critical components supporting the F/SCFs 1,2 [e.g. USAF AC17-01, DO-178C]. Pre- flight and/or pre-engagement built-in-test (BIT) ensures the system and all redundant elements are performing within acceptable tolerance levels. Monitoring redundant elements of the SCF in-flight protects against anomalous behavior unless the attack can create the same effects in multiple, redundant, and isolated elements simultaneously (common mode). Some common mode protection is provided by watch dog timers (WDT), which trigger a warm restart and initialize all input data to a predetermined value, if a process times out. [JSSG 2008, Mil-HDBK-516C]
    - Requirement 4.3 - All weapon system components containing CPI (CPI-1 and CPI-2) require the appropriate anti-tamper provisions. Configuration identification numbers are compared against the released weapon system configuration during maintenance, as well as during start-up and initiated BIT for SCF components. Cyclic Redundancy Checks and checksums also used to detect incorrect software versions and memory anomalies during BIT. **(Revalidate baseline including modificatio**n) [JSSG 2008, Mil-HDBK-516C]
    - Requirement 5.1 - Isolating redundant elements in safety/mission critical functions is “best practice” for military and commercial systems. Isolating F/SCF-1 and F/SCF-2, components, and wiring from less critical functions is standard practice. Partitioning is also standard practice for software components of varying criticality. **(Revalidate baseline including modificatio**n) [JSSG 2005, JSSG 2008, Mil-HDBK-516C]
    - Requirement 5.2 - Prioritization of MCF-2c, F/SCF-1, and F/SCF-2 based on failures is addressed in JSSG 2008 and Mil-HDBK-516C.
    - Requirements 6.1 and 6.2: interfaces will be monitored in accordance with requirement 7.1 and encrypted in accordance with requirement 3.1. **(Revalidate baseline including modificatio**n)
    - Requirement 7.1 to 7.3 - Monitoring, detection, and annunciating failures and/or anomalous behavior are required for all military and commercial F/SCF-1, F/SCF-2, and MCF-2c. Logging the failures is typically done in non-volatile memory internal to the system for retrieval post flight and/or on a data recorder function or maintenance system. **(Revalidate baseline including modificatio**n) [JSSG 2008, Mil-HDBK-516C, AC 25.1309-1A]
    - Requirement 8.1, 8.4, and 8.5 can be accomplished by fail-safe design practices identified in JSSG 2008, Mil-HDBK-516C, AC 25.1309-1A **(Revalidate baseline including modification)**

- Requirement 9.1 - This is addressed as part of the FTA, which includes the Safety Critical Functional Thread Analyses (SCFTA), Safety Hazard Analysis, Failure Modes and Effects Criticality Analysis (FMECA) and resulting Failure Modes and Effects Testing (FMET), and PNT certification for the upgraded EGI-M.
- Requirement 10.1 will need to be incorporated into the Tech Data to ensure continuous monitoring throughout the life cycle.

Request for Proposal and Planning (SSE Acq Guidebook, para 2.2, 2.3, 2.3.1, 3.1)

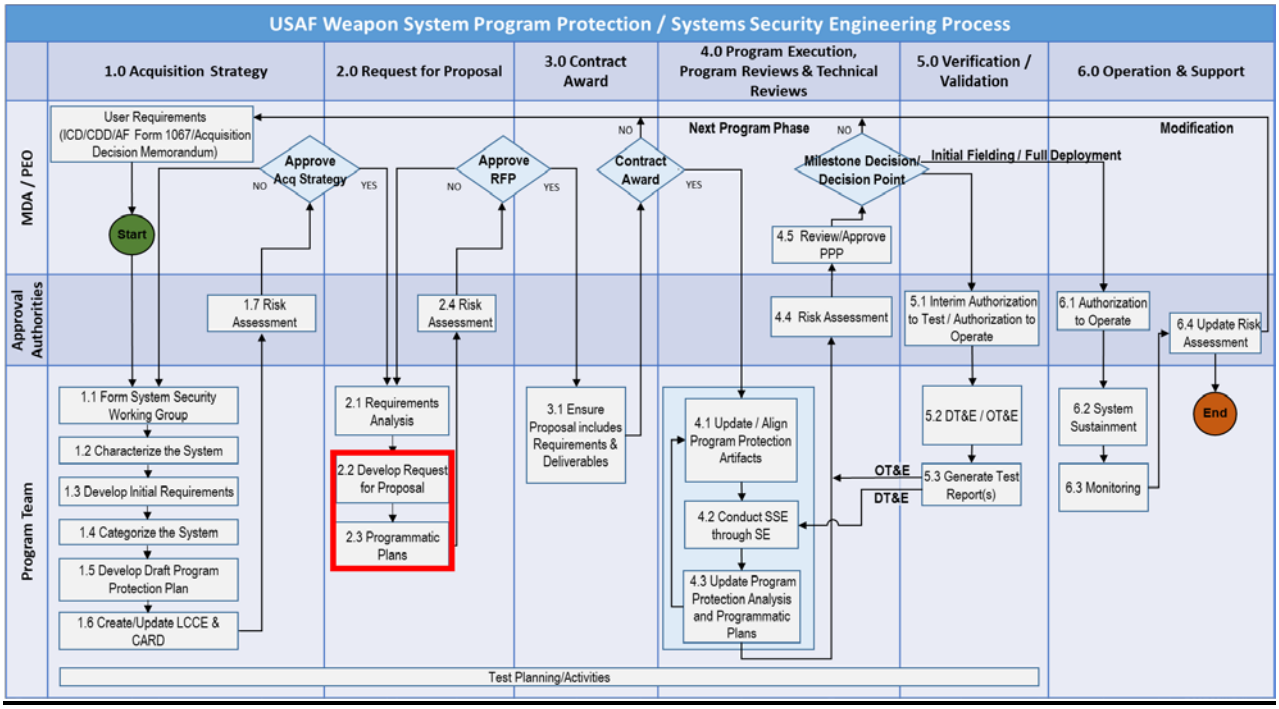


Figure D-22. PP/SSE Process – Develop Modification Request for Proposal

The proposal will contain program protection elements across most sections.to include the System Requirements Document (SRD), Statement of Work, Contract Data Requirements List (CDRL). Contract Clauses are included in the modification contract. No Section L or M is required, since the assumption is that the UAS prime will conduct the competitive selection for a new Resilient EGI (R-EGI).

- The Specification will contain the program protection requirements that were developed and analyzed in the Develop Initial Requirements and Analysis section above (see the system level requirements in the embedded worksheet in this section, and reference SSE Acq Guidebook, para 2.2).
- A security classification guide needs to be developed and approved for collateral and higher levels, if required for this modification. (SSE Acq Guidebook, para 2.2)
- As the Statement of Work is developed, the program protection elements identified in Attachment D-1 need to be considered for inclusion along with the associated CDRLs (provided in Attachment D-2). In many cases the CDRLs will be updates to the baseline program. (SSE Acq Guidebook, para 2.3)
- The main body of the modification contract needs to include the contract clauses addressed in Attachment D-3. (SSE Acq Guidebook, para 3.1)

When the Request for Proposal (RFP) is complete the engineering team needs to begin planning for the execution of the modification program. The engineering team should:

- Update Program level plans/guides (program protection plan, cybersecurity protection plan, Anti-Tamper plan, security classification guide, etc.
- Define any organization changes required, such as a dedicated navigation engineer and program manager and insure that the team is aware of their responsibilities.
- The risks developed at the end of the previous phase must be updated. Any new risks should be established and coordinated with the Prime Contractor team.
- Support should be provided to the program management team to gain release of the RFP.

When the proposals are submitted, they need to be reviewed to ensure that all requirements (SRD & SOW) / deliverables are addressed and evaluated in accordance to support contract award

Program Execution (through CDR)

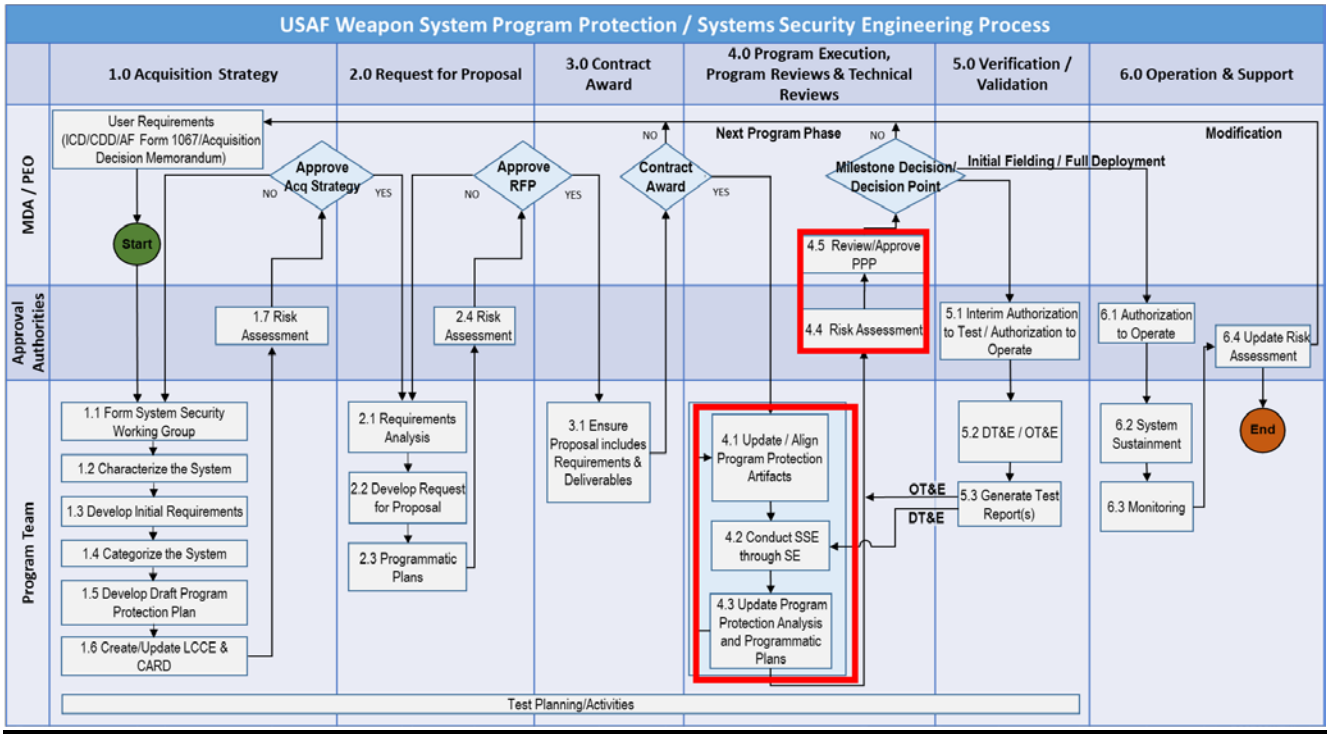


Figure D-23. PP/SSE Process – Contract Award through CDR

During the program execution phase, the modification to the system will be designed, built, and lab tested at the subsystem/software level and integrated via laboratory testing. Activities for a system modification in this portion of the PP/SSE Process parallel the activities for a new start program. Reference the previously discussed activities in the *Program Execution (Through CDR)* section and Figure D-14 in *Part 1: Aircraft System New Start Program* of this appendix.

System Design Considerations and Practices (SSE Acq Guidebook, para 4.1.2)

The following are overarching system design considerations and practices that should be evaluated as part of the systems engineering process used initial design and architecture definition. These also support CSA requirement 8.4.1.

- Aircraft Systems are not installed without rigorous safety assessments. Any system interconnection effects are integral to the safety assessment process (specific highlights below). The fail-safe design concept is inherent to approved designs. [ASISP Working Group – Final Report August 22, 2016]
- The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e., to ensure that major failure conditions are improbable and that catastrophic failure conditions are extremely improbable.
  - Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures.
  - Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.
  - Isolation of Systems, Components, and Elements so that the failure of one does not cause the failure of another. Isolation is also termed independence.
  - Proven reliability so that multiple, independent failures are unlikely to occur during the same flight.
  - Failure warning or Indication to provide detection and isolation.
  - Flight Crew Procedures for use after failure detection, to enable continued safe flight and landing by specifying crew corrective action.
  - Checkability: the capability to check a component's condition (e.g. start-up BIT, pre-engage or pre-mission IBIT, Maintenance BIT, fail over, backup navigation modes).
  - Error-Tolerance that considers adverse effects of foreseeable errors during modification design, test, manufacture, and operation (AC 25.13091A dated June 1988).

System Requirements Review / System Functional Review (SRR/SFR) (SSE Acq Guidebook, para 4.1.2, 4.1.3)

The first step in the design process is to understand and decompose the modification system and subsystem requirements – starting from the SRD, to the updated System Specification, down to existing and new Critical Item Development Specifications (e.g., R-EGI). This decomposition results in the subsystem requirements mapped to each of the 10 Cyber Survivability Attributes (CSA). These recommended subsystem requirements were further assessed and tailored as required. Ensure that each SSE subsystem requirement is traceable to a lower level requirement.

Systems Requirements Review / System Functional Review (SRR/SFR) exit criteria include:

- System Architecture Defined
- Updated FTA reviewed
- Critical Component / Critical Program Information (CC/CPI) analysis completed
- Anti-Tamper (AT) Plan updated
- Cybersecurity strategy defined
- Supply Chain Risk Management Plan included within the Security Plan

- SSE mapped to program documents (Systems Engineering Plan, Test and Evaluation Plan, Risk Management Plan and Life Cycle Sustainment Plan)
- Contractor Program Protection Implementation Plan delivered and reviewed
- Update Program Security Classification Guide(s)

Preliminary Design Review (PDR) (SSE Acq Guidebook, para 4.1.4)

From this point the requirements are decomposed into the components of the system establishing the allocated design. The identified security requirements must be examined at the PDR to ensure that the hardware and software design will protect the system IAW the plans in place. Exit criteria at the PDR include:

- System Architecture baselined
- Allocated requirements approved
- Select subsystem PDR actions and risks are flowed to the Weapon System Review.
- Systems Security Risks and Mitigations reviewed and updated
- Manufacturing sources associated with key CC/CPI identified
- Hardware and Software assurance levels defined for CC/CPI and documented in the design specification and SDP
- AT plan approved by Anti-Tamper Executive Agent (ATEA) and Program Executive Officer (PEO)
- Cybersecurity Strategy and Plan approved
- Initial attack path analysis is approved

The baseline criticality analysis has not changed from baseline. The Resilient EGI (R-EGI) remains Flight/Safety Critical and CPI. Also, the attack path analysis for the Dissemination of Battlefield Information has not changed, since the interfaces of critical components has not changed. The functional thread analysis and attack path analysis (**Table D-8a/Table D-8b and Table D-9**, respectively)

Table D-8a: Functional Thread Analysis Results for Dissemination of Battlefield Intelligence

Mission	Critical Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I,II,III,IV)
Dissemination of Battlefield Intelligence	Mission Planning **(MCF-2c1)**	Joint Mission Planning System	I
	Communications **(F/SCF-1; MCF-2c2a)**	C Band Data Link (including antenna) and SW	I
		Ku Band SATCOM	II
		UHF/VHF Voice Communications	III
	Vehicle Control **(F/SCF-1)**	Flight Control	I
		Propulsion System and SW	I
		Subsystem Controls	I
	Pilot Vehicle Interface **(F/SCF-1)**	Primary Flight Reference	I
		Pilot Controls	III
		Displays	I
	Sensors **(MCF-2c3; CPI-1a,1b,1c)**	EO/IR Sensor - Sensor Head **(CPI-1a)**	II
		SAR Radar - Transmit / Receive Modules **(CPI-1b)**	II
		SIGINT System - Mission Data File (MDF) and Digital Receiver **(CPI-1c)**	II
	Network Communications **(MCF-2c4, CPI-2)**	Communications Relay - Processor SW **(CPI-2)**	I
	Command and Control **(F/SCF-2)**	Ground Control Segment Processor	I
	Autonomous Navigation **(SCF-1; CPI-3)**	**Resilient Embedded GPS/INS** and Radar Altimeter (including antenna) and SW - Fiber optic gyros and antenna electronics **(CPI-3)**	I

Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible

Table D-8b: Functional Thread Analysis Results for NBC Treaty Compliance Monitoring

Mission	Critical Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I,II,III,IV)
NBC Treaty Compliance Monitoring	Mission Planning **(MCF-2d1)**	Joint Mission Planning System	I
	Communications **(F/SCF-1; MCF-2d2a)**	C Band Data Link (including antenna) and SW	I
		Ku Band SATCOM	II
		UHF/VHF Voice Communications	III
	Vehicle Control **(F/SCF-1)**	Flight Control	I
		Propulsion System and SW	I
		Subsystem Controls	I
	Pilot Vehicle Interface **(F/SCF-1)**	Primary Flight Reference	I
		Pilot Controls	III
		Displays	I
	Sensors **(MCF-2d3; CPI-1a,1d)**	EO/IR Sensor - Sensor Head **(CPI-1a)**	II
		Multi-Spectral Sensor Pod - Sensor Head **(CPI-1d)**	I
	Network Communications **(MCF-2d4, CPI-2)**	Communications Relay - Processor SW **(CPI-2)**	I
	Command and Control **(F/SCF-2)**	Ground Control Segment Processor	I
	Autonomous Navigation **(SCF-1; CPI-3)**	**Resilient Embedded GPS/INS** and Radar Altimeter (including antenna) and SW - Fiber optic gyros and antenna electronics **(CPI-3)**	I

Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible

The results of the attack path analysis results in the Subsystems containing CC/CPI and the Access Point assessment as shown in **Table D-9**.

Table D-9: Attack Path Analysis Results

	C Band Data Link	UHF/VHF Radio	Ku Band SATCOM	Flight Control Computer & SW	Engine Digital Controller & SW	Air Data Computer & SW	Resilient Embedded GPS/INS	EO/IR Seeker	SAR Array	SIGINT Processor SW	Multi-Spectral Sensor Pod	Primary Flight Display & SW	Pilot Controller	Mission Sensor Display & SW	Mission Planning Computer & SW
C Band Data Link					Encrypted Link	Encrypted Link		Encrypted Link	Encrypted Link	Encrypted Link	Encrypted Link	Encrypted Link			Encrypted Link
UHF/VHF Radio			VOIP Encrypted										VOIP Encrypted		
Ku Band SATCOM		VOIP Encrypted											VOIP Encrypted		
Flight Control Computer & SW	Encrypted Link					1553 and Discrete	1553 and Discrete								
Engine Digital Controller & SW	Encrypted Link			1553 and Discrete		1553 and Discrete									
Air Data Computer & SW				1553 and Discrete	1553 and Discrete										
Resilient Embedded GPS/INS	Encrypted Link			1553 and Discrete				1553	1553	1553	1553	Encrypted Link			
EO/IR Seeker	Encrypted Link						1553						Encrypted Link	Encrypted Link	
SAR Array	Encrypted Link						1553						Encrypted Link	Encrypted Link	
SIGINT Processor SW	Encrypted Link						1553						Encrypted Link	Encrypted Link	
Multi-Spectral Sensor Pod	Encrypted Link						1553								
Primary Flight Display & SW	Encrypted Link						Encrypted Link						Ethernet		
Pilot Controller	Encrypted Link	VOIP Encrypted	VOIP Encrypted									Ethernet		Ethernet	Encrypted Ethernet
Mission Sensor Display & SW	Encrypted Link												Ethernet		
Mission Planning Computer & SW													Encrypted Ethernet	Encrypted Ethernet	

Preliminary updates to impacted MIL-STD 1553, ethernet, and discrete interfaces are documented in configuration management controlled Interface Control Documents (ICD).

Updated risk assessment based on the cybersecurity requirements identified can be seen in **Figure D-24**. The integration of the Resilient EGI further mitigated baseline risk to a “1” for Likelihood and Consequence.

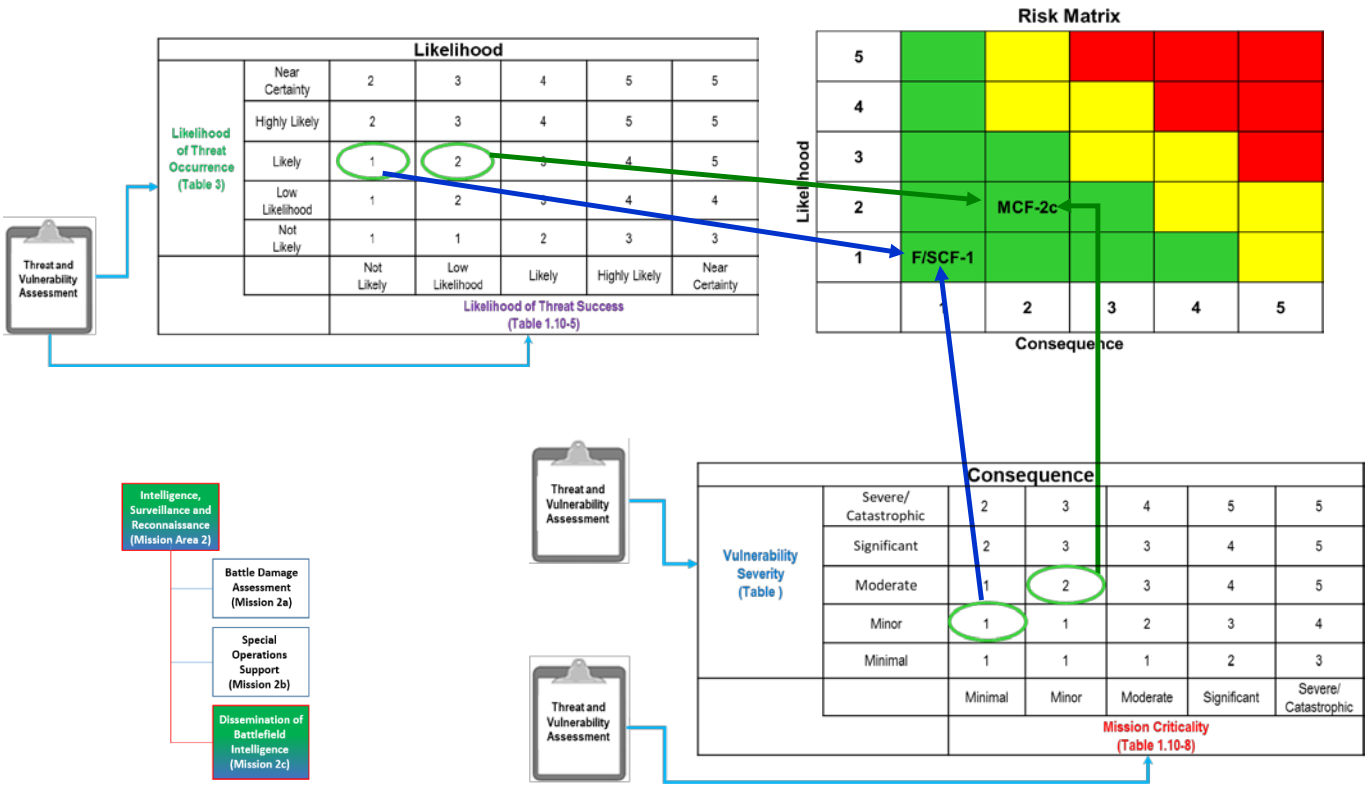


Figure D-24. Mitigated Risk for MCF-2c and F/SCF-1

Critical Design Review (CDR) (SSE Acq Guidebook, para 4.1.5)

The detailed HW and SW design completed. Exit criteria at the CDR include:

- Select subsystem CDR actions and risks are flowed to the Weapon System Review.
- TEMPEST Control Plan reviewed
- Modeling and Simulation accreditation validation / verification plan approved
- Hardware and Software design documentation baselined
- Updated FTA reviewed
- Attack path analysis updated, if required
- AT requirements updated
- CC/CPI updated
- Final updates to ICDs are approved
- SSE risks updated and mitigations updated
- SSE test plans and procedures completed and reviewed

Attachment D-1

MAE UAS STATEMENT OF WORK SECURITY TASKS

(SSE Acq Guidebook, para 2.3)

STATEMENT OF WORK	
1.0 Program Protection	
1.1	The contractor shall deliver a Program Protection Implementation Plan (PPIP). The contractor shall integrate the PPIP activities in the Integrated Master Plan/Integrated Master Schedule (IMP/IMS). The contractor shall derive requirements from the PPIP and put into specification(s), trace, and verify through the Systems Engineering Processes. Program Protection includes the following areas: Cybersecurity to include Trusted Systems and Networks (TSN), Cyber Resiliency, Anti-Tamper, and Information Protection. The contractor shall utilize modeling and simulations for verification of specifications. The contractor shall accredit and verify modeling and simulation used for closure of any specification requirements in accordance with MIL-STD-3022. All paragraphs below shall be contained in the PPIP. The Government shall be able to participate in all testing. In addition, the contractor shall allow the Government time in the laboratories and with the weapon system to conduct Penetration testing. The contractor shall conduct its own weapon system penetration testing and provide the test plan, procedures and reports (CDRLs 1, 2, 3, 4, 5, 6, 7, 8, 9, 34, 35, 36, and 37).
1.2	The contractor shall perform a Program Protection / Systems Security Risk Assessment of the requirements per section 1.10, Risk Management of the USAF Systems Security Engineering Acquisition Guidebook, utilizing the Systems Security Working Groups. These risks shall be part of the program risks. In addition, the contractor shall provide courses of action with cost details to get all risk to below medium (CDRLs 10 and 11).
1.3	The contractor shall report Cyber incidents (for all sections in the SOO/SOW) to the Government, IAW DFAR Clause 252.204-7012, (Safeguarding Covered Defense Information and Cyber Incident Reporting) via CDRL/DID, to the Defense Cyber Crime Center (DC3) via the DIBNet, and Joint Deficiency Reporting System. In addition, provide a root-cause, corrective-action report. The contractor shall establish and maintain an incident response infrastructure with identified membership and operating procedures to facilitate rapid response to cybersecurity incidents as documented in the contractor Security Plan/Security Assessment Plan (CDRLs 12 and 15).
1.4	The contractor shall participate in the Government-led IPTs or Systems 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 13 and 14).
1.5	The contractor shall perform 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 to determine likely avenues of cyber-attack. The contractor shall perform a covert channel analysis to identify those aspects of communications within the weapon system that are potential avenues for covert storage and/or timing channels (CDRL 38).

2.0 Cybersecurity	
2.1	The contractor shall provide a Cybersecurity Strategy (to include TSN and Cyber Resiliency) and data to support the development of the Security Plan. The contractor shall provide a Security Assessment Plan, a Security Assessment Report, and a Plan of Action and Milestones POA&M. The contractor shall ensure the weapons system's configuration has been baselined and documented to meet the cyber-requirements (CDRLs 3, 4, 5, 15, 16, 23, 42, 43, and 44).
2.2	The contractor shall provide the Criticality Analysis for Safety Critical Functions, Mission Critical Functions, and Critical Program Information (for all CPI and Anti-Tamper, see CPI/AT section) thread, IAW DoDI 5200.44, 5200.47, and 5000.39; Airworthiness Circular AC-17-01; and the USAF Combined Process Guide for CPI and CC Identification. In addition, the contractor shall ensure the Failure Modes Effects Analysis (FMEA) trace to the Criticality Analysis, which are documented in the Failure Modes Effects Criticality Analysis (FMECA). The contractor shall design the system with redundant/reverse redundant capability(ies) to reduce and eliminate single point of failure of all safety critical functions and mission critical functions based on risk (CDRLs 17, 18, and 19).
2.3	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, and traced to the Bill of Materials to the lowest critical components throughout the EMD phase. The contractor shall update design via system engineering processes to ensure above-medium risk components are not in the system (CDRL 20).
2.4	The contractor shall allocate system security and resiliency requirements to architectural entities and system elements, if required. The contractor shall trace system architecture design to the requirements derived from the agreed to SCTM NIST 800-53R4 controls (SP/SAP) IAW DoDI 8500.01 and DoDI 8510.01 and TSN per DODI 5200.44, AT per DODI 5200.44 and 5200.39, and Resiliency requirements. The contractor shall allocate requirements to the Safety Critical Functions (SCFs), Mission Critical Functions (MCFs), and CPI commensurate with operational-risk categorization. The contractor shall utilize the lower level requirements located in Attachment 1 of the USAF Systems Security Engineering Acquisition Guidebook and provide a requirements traceability matrix. The contractor shall ensure integration and verification that SCFs, MCFs, and CPI have the appropriate segregation and diverse redundancy in the architecture to complete the mission (resiliency), see requirement section for more information. In addition, the Architect Design Document shall include an analysis of any other systems'/subsystems' interconnects/interfaces that are not SCF, MCF, CPI/AT. If there are interconnects/interfaces, the Architect Design Document shall ensure the appropriate segregation and diverse redundancy is maintained for the SCF, MCF, and CPI/AT (CDRLs 7, 21)
2.5	The contractor shall ensure all new hardware, with special emphasis on lowest 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, IAW the current version of CNSSD No. 505 and NIST SP 800-161, to mitigate supply chain risk. The contractor shall ensure that no critical components procured are on the Section 806 List or the Section 2339a list in the Supplier Performance Risk System (SPRS). In addition, the contractor shall develop and implement a Counterfeit Parts Prevention program 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 (CDRLs 22, 23, 31, 39, 40, and 41)

2.6	The contractor shall provide a Software Development Plan (SDP) 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 based on the Functional Thread Analysis. 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 (CDRLs 3 (STP), 5 (STR), 23, 24, 25, 26, 32, 43, 44, and 45)
2.7	The contractor shall develop an NSA-approved Key and Certificate Management Plan (KCMP) for each cryptographic system. 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 Section 2.3.2.A (CDRL 27).
2.8	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 28).
2.9	The contractor shall provide all information required for the program office to obtain Interim Authority To Test (IATT) and Authority To Operate (ATO). (CDRL 29).
3.0 Critical Program Information (CPI) / Anti-Tamper (AT)	
3.1	The contractor shall develop and implement Anti-Tamper (AT) hardware and software 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 AT Desk Reference and Anti-Tamper Technical Implementation Guide (TIG), 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 30).
4.0 Security Management / Information Protection	
4.1	The contractor shall develop and maintain a security program to comply with requirements of the Government-provided Contract Security Classification Specification, DD Form 254.
4.2	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 33).
4.3	The contractor shall provide Operations Security (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.
4.4	The contractor shall be compliant to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 in accordance with DFARS, Provision 252.204-7008 (CDRL 15).
4.5	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.

4.6	The contractor shall develop and store in a secure facility all DoD technical data (e.g., source code), and computer software in the possession or control of non-DoD entities on non-DoD information systems in protected means through segregation control (e.g., firewall, isolated network, etc.) to prevent connections to the GIG and document meeting this requirement in the contractor Security Plan (CDRL 15).
4.7	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) unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer (DoD CIO). (CDRL 23).

Attachment D-2

MAE UAS SYSTEM SECURITY CDRLS

(SSE Acq Guidebook, para 2.3)

CDRL	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)
1 Program Protection Implementation Plan (PPIP) **(Mod: Update)**	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 • 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 • Update annually	Follow the newest OSD PPP template
2 Specification **(Mod: Update and New)**	Program-Unique Specification Documents	DI-SDMP-81493	Standard program delivery	
	Interface Requirements Specification (IRS)	DI-IPSC-81434	• Preliminary draft due 30 days prior to CDR • Updates due 60 days prior to the associated PCA for each CI/CSCI • Draft due 30 days prior to SVR • Final due 30 days after Government approval	
3 Test Plan for all testing Laboratory, Ground, and Flight **(Mod: Update and New)**	Test Plan	DI-NDTI-80566	• 150 days prior to test • 60 days prior to Test Readiness Review	
	Test and Evaluation Program Plan (TEPP)	DI-NDTI-81284	• 150 days prior to test • 60 days prior to Test Readiness Review	

CDRL	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)
	Software Test Plan (STP)	DI-IPSC-81438	• 150 days prior to test • 60 days prior to Test Readiness Review	
4 Test Procedures for all testing Laboratory, Ground, and Flight **(Mod: Update and New)**	Test Procedure	DI-NDTI-80603	• 150 days prior to test • 60 days prior to Test Readiness Review	
5 Reports for all Analysis, Inspection, Demonstration and Test	Software Test Report (STR)	DI-IPSC-81440	• Quick Look Report for 30 days after test • Final 60 days after test of closure of specification • 150 days prior to CDR, FCA, SVR	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)].*
	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	
6 Integrated Master Schedule (IMS) **(Mod: Update)**	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	
7 Traceability Matrix **(Mod: Update)**	Technical Report Study/Services (addressing Traceability Matrix)	DI-MISC-80508	90 days prior to PDR, CDR, TRR, FCA, SVR	

CDRL	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)
8 Models, Tools and Source data for the Digital Engineering **(Mod: Update)**	Technical Report Study/Services (addressing Models, Tools and Source data for the 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.
9 Interface Control Documents (ICDs) **(Mod: Update)**	Interface Control Document (ICD)	DI-SESS-81248	150 days prior to CDR, FCA, SVR	
10 Risk Management **(Mod: Update)**	Contractor's Risk Management Plan	DI-MGMT-81808	Standard program delivery	
	Security Vulnerability Analysis	DI-MISC-80841	Standard program delivery	
	Technical Report Study/Services (addressing Risk Assessment Report)	DI-MISC-80508	Standard program delivery	
11 COAs with Cost Technical Report **(Mod: If required)**	Technical Report Study/Services (addressing the Cost Technical Report)	DI-MISC-80508	Standard program delivery	
12 Cyber Incidents **(Mod: Update)**	Technical Report Study/Services (addressing the Incident, Root Cause, and Corrective Action)	DI-MISC-80508	• Draft report 24 hours after incident • Final report 10 days after incident	
13 Meeting Minutes and Action Items	Conference Minutes	DI-ADMN-81250	30/60 days after meeting	
14 Agenda	Conference Agenda	DI-ADMN-81249	30 days prior to meeting	

CDRL	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)
15 Contractor Security Plan **(Mod: Update)**	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	
16 Security Assessment Report **(Mod: Update)**	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, 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, architecture 120 days prior to Authority To Authorize (ATO) • Update as required	
17 Criticality Analysis **(Mod: Update)**	Technical Report Study/Services (addressing Criticality Analysis)	DI-MISC-80508	• Functional Analysis 60 days prior to SRR/SFR • Thread analysis 60 days prior to PDR • Update 60 days prior to CDR • Update as required	Report shall address the Mission Critical Function Thread Analysis, Safety Critical Function Thread Analysis and Critical Program Information Thread Analysis
18 Failure Mode, Effects Analysis (FMEA) **(Mod: Update)**	Technical Report Study/Services (addressing FMEA)	DI-MISC-80508	• Functional Analysis 60 days prior to SRR/SFR • Thread analysis 60 days prior to PDR • Update 60 days prior to CDR • Update as required	
19 Failure Mode, Effects & Criticality Analysis (FMECA) **(Mod: Update)**	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	

CDRL	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)
20 Critical Component Information **(Mod: Update)**	Technical Report Study/Services (addressing Critical Components) following template in the PPP (System/Subsystem, Manufacture, P/N, etc.)	DI-MISC-80508	• 30 days after known • 60 days prior to PDR • 60 days prior to CDR	
21 Architect Design Document **(Mod: Update)**	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)	
22 Manufacturing Plan **(Mod: Update)**	Customized Microelectronics Devices Source Protection Plan	DI-MGMT-81763	Standard program delivery	
	Counterfeit Prevention Plan	DI-MISC-81832	Standard program delivery	
	Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report	DI-QCIC-80125	Standard program delivery	
	Technical Report Study/Services (addressing the Manufacturing Program Plan)	DI-MISC-80508	Standard program delivery	
23 Security Assessment Plan **(Mod: Update)**	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	

CDRL	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)
24 Software Development Plan **(Mod: Update)**	Software Development Plan (SDP)	DI-IPSC-81427	• Preliminary draft 30 days prior to System Requirements Review (SRR) • Draft due 45 days after System • Functional Review (SFR) • Final due 30 days after Government approval • After Government approval, contractor shall submit subsequent revisions to address contractor proposed changes	
25 Software Requirement Specifications **(Mod: Update and New)**	Software Requirements Specification (SRS)	DI-IPSC-81433	• Preliminary draft for each CSCI due 30 days prior to SFR • Updates due 30 days prior to both PDR and CDR • Draft due 60 days prior to each associated CSCI's FCA • Final due 30 days after Government approval • Proposed changes to approved specification due 30 days prior to SVR for approval	
	Software Product Specification (SPS)	DI-IPSC-81441	• Preliminary draft for each CSCI is due 30 days prior to the associated PCA • Draft for each CSCI is due 30 days after associated PCA for each CSCI • Final due 30 days Government approval • Proposed changes to approved specifications due 30 days prior to PCA for Government approval	
26 Software Test Plans and Procedures **(Mod: Update and New)**	Software Test Description (STD)	DI-IPSC-81439	• 150 days prior to test • 60 days prior to Test Readiness Review	
	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	

CDRL	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)
	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	
	System/Software Integration Laboratory (SIL) Development and Management Plan	DI-SESS-81770	• 150 days prior to test • 60 days prior to Test Readiness Review	
27 Key and Certification Management Plan (KCMP) **(Mod: Update)**	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	
28 TEMPEST Control Plan **(Mod: Update)**	TEMPEST Control Plan	DI-MGMT-81026	• 150 days prior to test • Final 30 days after test completion	
	TEMPEST Test Plan	DI-EMCS-81683	• 150 days prior to test • Final 30 days after test completion	
	TEMPEST Test Evaluation Report	DI-EMCS-81684	• 150 days prior to test • Final 30 days after test completion	

CDRL	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)
29 Data Accession List **(Mod: Update)**	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	
30 AT Plan **(Mod: Update)**	Technical Report Study/Services (addressing the AT Plan (PPIP 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 Verification and Validation (V&V) Plan 60 days prior to PDR • Final V&V Plan and 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	
	Technical Report Study/Services (addressing the Anti-Tamper (AT) Verification Plan)	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 Verification and Validation (V&V) Plan 60 days prior to PDR • Final V&V Plan and 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	

CDRL	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)
	Technical Report Study/Services (addressing the Anti-Tamper (AT) Verification Report)	DI-MISC-80508	• Initial Verification and Validation (V&V) Plan 60 days prior to PDR • Final V&V Plan and 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	
	Technical Report Study/Services (addressing the Anti-Tamper (AT) Plan)	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 Verification and Validation (V&V) Plan 60 days prior to PDR • Final V&V Plan and 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	
31 Information Systems Security (INFOSEC) Anonymity Plan (IAP) **(Mod: Update)**	Information Systems Security (INFOSEC) Anonymity Plan (IAP)	DI-MGMT-81717	Standard program delivery	

CDRL	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)
32 Information Security (INFOSEC) Boundary Configuration Management Plan **(Mod: Update)**	Information Security (INFOSEC) Boundary Configuration Management Plan	DI-SESS-81343	Standard program delivery	
33 Operations Security (OPSEC) Plan **(Mod: Update)**	Operations Security (OPSEC) Plan	DI-MGMT-80934	Standard program delivery	
34 DoD Modeling and Simulation (M&S) Accreditation Plan **(Mod: Update)**	Department Of Defense (DoD) Modeling and Simulation (M&S) Accreditation Plan	DI-MSSM-81750	60 days prior to PDR Update as required	
35 DoD Modeling and Simulation (M&S) Accreditation Report **(Mod: Update)**	Department Of Defense (DoD) Modeling and Simulation (M&S) Accreditation Report	DI-MSSM-81753	60 days prior to CDR Update as required	

CDRL	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)
36 DoD M&S Verification and Validation (V&V) Plan **(Mod: Update)**	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	
37 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	
38 Attack Path Analysis Report **(Mod: Update)**	Technical Report Study/Services (addressing Attack Path Analysis)	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	
39 Acceptance Test Plan **(Mod: Update)**	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	
40 Acceptance Test Procedure **(Mod: Update and New)**	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	

CDRL	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)
41 Acceptance Test Report	Acceptance Test Report (ATR)	DI-QCIC-81891	• 30 days after test completion	
42 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	
43 Configuration Management Plan **(Mod: Update)**	Technical Report Study/Services (addressing overall System Configuration)	DI-MISC-80508	• 60 days prior to PDR • Update as required	
44 Configuration Management Report **(Mod: Update)**	Technical Report Study/Services (addressing overall System Configuration)	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	
45 Software Development Description **(Mod: Update)**	Software Design Description (SDD)	DI-IPSC-81435	• Submittal for each CSCI due 30 days prior to CDR • Final submission for each CSCI due 60 days after CDR	

Attachment D-3

MAE UAS CONTRACT CLAUSES

(SSE Acq Guidebook, para 3.1)

CONTRACT CLAUSES	
Part 52.204-2 Security Requirements (AUG 1996)	Applies to the extent that the contract involves access to information classified Confidential, Secret, or Top Secret. 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. Requires the contractor to include this clause in all subcontracts.
Part 52.204-21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)	Applies to the extent that the contract involves access to information classified Confidential, Secret, or Top Secret. 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. Requires the contractor to include clause in all subcontracts, if access to classified information is required.
Part 52.204-9 Personal Identity Verification of Contractor Personnel (JAN 2011)	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. Requires the contractor to account for all forms of Government-provided identification issued to the contractor employees in connection with performance under this contract.
Part 52.239-1 Privacy or Security Safeguards (AUG 1996)	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. Requires immediate notification if existing safeguards have ceased to function and/or if either the Government or the contractor discovers new or unanticipated threats or hazards.
252.204-7000 Disclosure of Information (Oct 2016)	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.
252.204-7008 Compliance with Safeguarding Covered Defense Information Controls (OCT 2016)	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 NISTSP 800-171.

CONTRACT CLAUSES	
252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (OCT 2016)	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 (OCT 2016)	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.
252.239-7000 Protection Against Compromising Emanations (JUN 2004)	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. Requires protection against compromising emanations. Requires the contractor to provide a TEMPEST accreditation date.
252.239-7001 Information Assurance Contractor Training and Certification (JAN 2008)	Requires contractor personnel accessing information systems to have the proper and current information assurance certification to perform information assurance, IAW DoD 8570.01-M. Requires the Government to ensure that the certifications and certification status of all contractor personnel is identified, documented, and tracked.
252.239-7018 Supply Chain Risk (OCT 2015)	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. 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. 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)	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)	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.
5352.215-9000 Facility Clearance (MAY 1996)	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).

Attachment D-4

REQUEST FOR PROPOSAL (RFP) SECTION L AND SECTION M

(SSE Acq Guidebook, para 3.2, 3.3)

SECTION L - SSE INSTRUCTIONS TO OFFEROR
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 Statement of Objective (SOO), Statement of Work (SOW), Systems Requirement Document (SRD), and Specification (Spec). The offeror's narrative shall include: 1. A Cybersecurity Strategy (to include Trusted Systems and Networks per DoDI 5200.44) that identifies the offeror's strategy to achieve 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) 800-53R4 controls per DoDI 8500.01 and DoDI 8510.01). 2. Cyber Resiliency techniques and approaches as required by the SOO/SOW, SRD/Spec, SP/SAP, and Architecture. 3. A description of the Anti-Tamper (AT) Plan in accordance with DoDI 5200.39 and 5200.47. 4. Information Protection as required by the DD Form 254 and Security Classification Guide. 5. 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. 6. 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.
SECTION M - SSE EVALUATION CRITERIA
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.

Attachment D-5

REFERENCES

[1] Ref: Air Force Association, http://secure.afa.org/grl/pdfs/AF_ISR.pdf

[2] AIR COMBAT COMMAND CONCEPT OF OPERATIONS FOR ENDURANCE UNMANNED AERIAL VEHICLES, dated 3 Dec 1996 - Version 2, https://fas.org/irp/doddir/usaf/conops_UAS/

[4] United States Air Force Combined Process Guide for Critical Program Information (CPI) and Critical Component (CC) Identification, VERSION 1.1, dated 8 May 2018

[5] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[6] Cyber Survivability Endorsement Implementation Guide (CSEIG) Volume I, Version 1.01

[7] MIL-HDBK-516C, Airworthiness Certification Criteria

[8] Joint Service Specification Guide (JSSG) 2006, Aircraft Structures Add 516, JSSG 2008

[9] Systems Security Engineering Acquisition Guidebook, Ver 1.4

[10] FAA AC 25.13091A, System Design and Analysis

[11] Aircraft Systems Information Security Protection (ASISP) Working Group Final Report (2016)

APPENDIX E – Sample Program Protection Plan (PPP)

Vehicle
Program Protection Plan

Supporting Milestone C

05 August 2019

FOREWORD

This Program Protection Plan (PPP) provides protection guidance for a generic sport utility vehicle (SUV) program, henceforth known as the Vehicle. It offers Program Managers (PM), and others to include industrial partners, a means to protect the program from its inception to its demilitarization. This PPP is intended as a consolidated security desktop reference and training tool.

The purpose of this plan is to identify elements of the program, classified or unclassified, that require protection to prevent the unauthorized disclosure or inadvertent transfer of Critical Program Information (CPI) as defined in "*Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation",* Department of Defense Instruction (DoDI) 5200.39, 28 May 2015 Incorporating Change 2, 15 Oct 2018; and to identify Mission critical Functions (MCF) and their components and protective countermeasures In Accordance With (IAW) *"Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)",* DoDI 5200.44, 15 October 2018. This PPP incorporates risk management and threat-based countermeasures to provide the cost-effective protection of the Vehicle program's effectiveness throughout its acquisition and operational life-cycle phases to include its demilitarization. This PPP template follows the outline, content and formatting required by DoDI 5000.02 and DoDI 5200.39, as delineated by the Deputy Assistant Secretary of Defense, Systems Engineering, "Program Protection Plan Outline & Guidance", Version 1.0 dated July 2011.

This PPP is effective upon its formal release and is designed for use by all programs, field activities and matrix-support personnel at all government and contractor locations. This plan contains information that is FOR OFFICIAL USE ONLY (FOUO) and is exempt from its mandatory disclosure under the Freedom of Information Act; exemptions 1, 3 and 5 pertain.

APPROVED BY:

Name Milestone Decision Authority	Approval Date

SUBMITTED BY:

_____ _____

Name Date
Program Manager

CONCURRENCE:

_____ _____

Name Date
Program Executive Officer or Equivalent

COMPONENT APPROVAL:

[Required for programs with OSD approval (ACAT ID, IAM, etc.)]

_____ _____

Name Date
Component Acquisition Executive

Table of Contents

1.0 Introduction

NOTE

After each main section heading, a table with black column headers will show what Contract Data Requirements List (CDRL) line items and USAF Weapon System PP/SSE Guidebook section (or WBS line) are addressed therein.

After each paragraph that references a CDRL, the associated USAF Weapon System PP/SSE Guidebook section number and CDRL # will be given, as: **[PP/SSE GB Section, CDRL #] (e.g. [App A 2.3.1 A, 1])**.

Table 1-1 Applicable CDRLs this Section

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 2.3.1 A	CDRL 1	60d > ACA	60d < PDR	60d < CDR	Annually
Appendix A, 2.3.2 B	CDRL 19	60d <	60d < PDR	60d < CDR	As Required
Appendix A, 2.3.2 C	CDRL 20	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 1.2.1	Acquisition Strategy, MBCRA	-	-	Pre-MS A	As Required
Appendix A, 1.1.1	ICD/CDD	-	-	Pre-MS A	As Required
Appendix A, 2.1	Architectures and Interface Control	-	-	Pre-SETR Events	As Required (e.g. ECP, SEMP)
WBS 2.3	Programmatic Plans	-	-	As Required	As Required
Appendix A, 1.7	Information Support Plan (ISP)	-	Pre-RFP	Pre-MS B	CDR
Appendix A, 2.3.2 D	CDRL 21	60d < SRR/SFR	60d < PDR	60d < CDR	As Required
Appendix A, 2.3.1 C	CDRL 11	-	-	Pre-MS A	As Required

The purpose of this Vehicle Program Protection Plan (PPP) is to incorporate cyber survivability safeguards into a state-of-the-art American-manufactured vehicle that is equipped with multiple automated functions and features while remaining focused on improving the occupants safe and entertained.

The vehicle's System of Systems (SoS) range from Adaptive Cruise Controls (ACC), Forward Collision Warning Plus (FCW+), Lane Departure Warning (LDW+), Park Assist System (PAM) to Anti-Theft (PATS), Tire Pressure Monitoring System (TPMS), Remote Keyless Entry/Start (RKE), Bluetooth, Wi-Fi, and various Telematic, Internet and driver/passenger applications.

This updated PPP will identify Critical Program Information (CPI) and Critical Components (CCs) associated with the vehicle's program, CPI and CC vulnerabilities to the Vehicle and its mission, threats to CPI or CCs, and the countermeasures in place to mitigate the risk of compromise of CPI or CCs through the vehicle's SoS life-cycle.
[App A Section 2.3.2 B, 19] [App A Section 2.3.2 C, 20]

This PPP will be used primarily by the Vehicle Program Managers (PM) and modification engineers to help identify the impact of existing CPI and/or CCs, and identification of new CPI or CCs due to system upgrades through the system's life cycle. This PPP will also be used by vehicle engineers to assist in the SoS assessment and authorization progress associated with technical modifications and compliance with International Organization for Standardization (ISO 26262) and Society of Automotive Engineers (SAE) J3061 Industrial standards.

The PPP and any associated documents will be marked and controlled in accordance with the program's Security Classification Guide (SCG). The PPP will be maintained and updated by the Vehicle Program Office (PO), and will be reviewed annually to validate threats, vulnerabilities, and countermeasures (see Table 1-2). PPP updates, as required, and prior to every Milestone Decision Authority (MDA) decision point and Systems Engineering Technical Review (SETR), but not to exceed every three (3) years. Further, this PPP will be updated by changes to the acquisition program status and in response to security threats, changes to the projected threat, or in the event of potential loss or compromise of any part of the Vehicle's operational, safety and entertainment systems. Other updates shall take place as deemed necessary by the Vehicle PM or Program Executive Officer (PEO).

Any PPP should be classified by content. Threat and vulnerability information is commonly classified at SECRET or above. Detailed descriptions of CPI and critical functions/components may also be classified. The program Original Classification Authority is responsible for determining appropriate classification of the PPP and related information. The PO may opt to reference some tables (e.g. threats, vulnerabilities) as classified appendices.

The authority for all updates to the PPP will be the Milestone Decision Authority or their designated representative. Delegation of update authority to the designated representative will be made in writing. Any changes to the existing contractor Program Protection Implementation Plan (PPIP) that directly relates to the PO PPP objectives must be vetted through the Government Contracting Officer. Other interested parties, such as supporting application developers, resellers, or vehicle contractors may provide recommendations for updates to this PPP through the Vehicle PM.
[App A Section 2.3.1 A, 1]

Table 1-2 Update Record / Update Record

Revision Number	Date	Changes	Approved By
1.0	8 April 2010	Original Document	
2.0	7 April 2019		

1.1 Technology/System Description

The Vehicle Program is an ACAT 1D, post-Milestone B program. The program is currently in its Low Rate Initial Production (LRIP) phase of pre-Milestone C. At the conclusion of this LRIP phase, the Vehicle will transition to its Full Rate Production phase. Table 1-2 provides to the latest Acquisition Strategy supporting documentation.

Table 1.1-1 Technology / System Description

Program Name	ACAT Level	Impact Value	Last Milestone
Vehicle	1D	Low	12 Sep 2012
Vehicle Modernization	1D	Low	

Functional Performance and Safety Requirements:

The Vehicle's primary mission is transporting the driver and five to six passengers safely using self-driving functions at any time in all-weather conditions. Self-Driving functions consist of the: Adaptive Cruise Control (ACC), Park Assist System (PAM), Lane Departure Warning Plus (LDW+) and Forward Collision Warning Plus (FCW+) systems. All occupants need to be entertained while inside the vehicle with fully automated functionality, as possible. These Capability Based Requirements (CBR)-based, Key Performance Parameters (KPP) to achieve this primary mission are:

KPP 1: Passenger Capacity - The system shall transport five people safely.
(Threshold 5 people; Objective 6 people)

KPP 2: Day/Night Operations - The system shall be operable all 24 hours in a day.
(Threshold=Objective)

KPP 3: All-Weather - The system shall be operable in all climate weather.
(Threshold=Objective)

KPP 4: Self-Driving: The system shall be capable of "self-driving."
(Threshold=Objective)

KPP 5: System Survivability (SS) - The system shall be able to maintain critical capabilities under applicable threat environments.
(Threshold=Objective)

KSA 1: Infotainment - The system shall be capable of providing entertainment to all occupants. (Threshold=Objective)

Exempting the existing Key System Attributes (KSA) and with no other new design Attributes, the KPP-related
Pillar-related Cyber Survivability Attributes (CSA) for full-rate production are documented in Appendix F.

[App A Section 1.2.1, Acquisition Strategy, CDD, MBCRA Input] [App A Section 1.1.1, ICD/CDD]

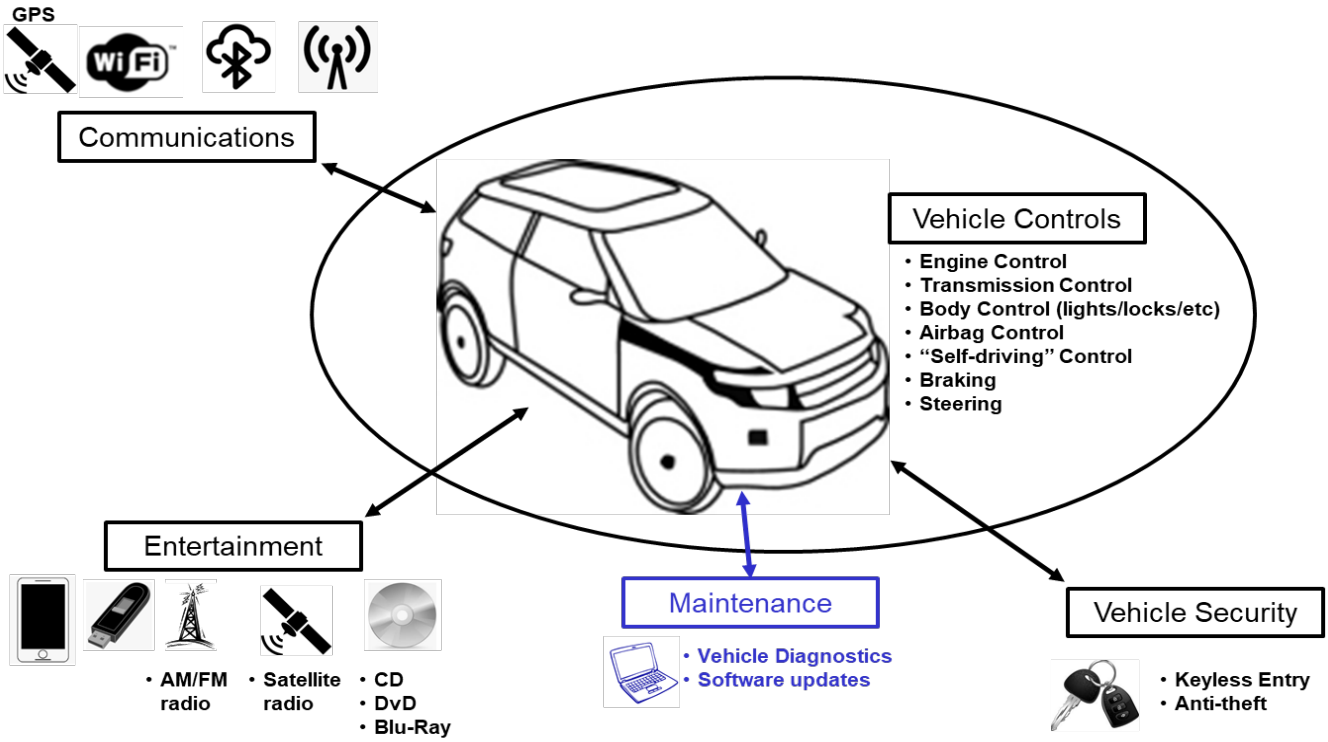


Figure 1.1-1 Vehicle OV-1

Vehicle Operational Viewpoint:

Operationally, the Vehicle will accomplish these missions primarily through a global mission environment of paved and unprepared roads and under all weather conditions. Figure 1.1-1 depicts the Vehicle mission with a system interface that includes controls (e.g. Braking & Steering, Motion & Positioning Sensors, Transmissions & Navigation and Entertainment System) and Communications (e.g. Bluetooth; GPS: Navigation and Internet/PSTN & WiFi). Steering includes an auto-parking capability and an integration of the engine, transmission and steering control systems.

For the mission of transporting passengers with no cargo in the rear of the cabin and the luggage rack on the Vehicle's roof, the Mission Critical Functions (MCF) are: global/world-wide operations; paved and un-prepared roads; and all weather transportation capability. The Vehicle supports an additional mission of transporting cargo in its internal rear bay with no passengers and/or with cargo in its internal rear bay with a front seat passenger, as well as, providing the passenger and Vehicle secondary capabilities of communication, entertainment and environmental monitoring.
[App A Section 2.1, Architectures and Interface Control]

Systems-Systems Vehicle Network Architecture

The Vehicle Controller Area Network (CAN) buses are Vehicle CAN C and CAN Interior High Speed (HIS) standards designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. These connected Local Replaceable Units (LRU) consist of the Engine Control Units (ECU), an AM/FM radio with USB2 and wireless and Bluetooth communications capabilities, and a proprietary internet cloud-Access Point (AP). Figure 1.1-2 illustrates the Vehicle's network architecture at a Tier 1, high-level.

There are 4 independent network buses: the CAN IHS, the CAN-C and Diagnostic CAN-C, the Local Interconnect Network (LIN). The LIN-Bus is a small, relatively slow and inexpensive network compared to the Controller Area Network (CAN-Bus). LIN is used mostly for Vehicle electrical systems. The CAN IHS is mislabeled as it is only a 125 kbps bus used for communications between the dashboard and the radio, for example. The Diagnostic CAN-C and CAN-C buses run at 500 kbps. The diagnostic bus primary function is obviously to run automated and manually selected tests on the Vehicle interconnected LRUs. The CAN-C bus ties together the engine, brakes, airbags etc. The main threat to this network stems from the connection between the radio, that functions as the Vehicle head control unit, and the other Vehicle buses.

The Body Control Module (BCM), a central organizational module for the Vehicle designed to streamline the manufacturing and troubleshooting aspects of electronic modules by housing the modules into one, central unit instead of each function having its own device, as well as, coordinating the operating functions of many non-engine related ancillary items like the Vehicle security features offers a penetration point from an external threat agent.

The access to the radio allows the exploitation of the ECUs through multiple probabilistic vector attack pathways, such as the cell phone or Bluetooth interfaces. From these two penetration points, a gateway opens to the CAN buses, and hence the ability to send messages from the Vehicle head control unit to every LRU tied to these interconnected buses.

[WBS 2.3, Programmatic Plans] [App A Section 1.7, Information Support Plan (ISP)] [App A Section 2.3.2 D, 21]

Cyber Survivability Risk Category (CSRC):

Based on the aforementioned cyber vulnerabilities, a CSRC3 level can be assessed against the Vehicle network architecture. Beyond controlling access to the current buses through communication pathways, the need for redundancy if any LRU is "bricked" by an external threat, monitoring the architecture for unusual anomalies, and an ability to reset any function and/or feature deemed compromised are design changes for the Low Rate Production Vehicles before stepping into its full rate commercial production schedule this year.

Program Information.

Table 1.1-2 shows as the maturity of the Vehicle design progressed and its vulnerabilities were realized, its interconnection to external supporting networks via the proprietary Cloud posed a threat and an elevated impact value of High status. The impact value should be reviewed and updated annually, or as required.

Table 1.1-2 Program Information

Program Name	ACAT Level	Impact Value	Last Milestone
Vehicle Block 1	1D	Low	12 Sep 2012
Vehicle Block 2	1D	Moderate	8 Feb 2015

1.2 Program Protection Responsibilities

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 1.1.2	High-Performance Team (HPT)	Pre-RFP	-	-	-
WBS 1.1.1	Appoint Personnel to SSWG / appropriate IPT	Pre-RFP	-	-	-

The PPP development starts at the highest levels of the Department of Defense (DoD) down through the United States Air Force (USAF) Headquarters for Acquisition (SAF/AQ); and in particular with regards to the High Performance Team (HPT), as per AFI 10-161.

High Performance Team (HPT):

HPT membership is made up of core and support representatives who are Subject Matter Experts (SMEs). The HPT prime mission is to delineate achievable, executable and affordable capabilities at optimal cycle time to the warfare fighter. The HPT translates customer requirements and their associated capabilities and desired effects into KPP, Key System Attributes (KSA), and/or Attributes. From these, the HPT provides user inputs to the Safety critical Functions (SCFs), MCFs, and functions associated with Critical Program Information (CPI) to the top-level architecture and the Cyber Survivability Attributes (CSA), appropriately. These inputs are flowed down to the respective Program Executive Offices (PEO) for their eventual realization as weapon systems and/or services.

The Vehicle PM is responsible for the development, approval, and implementation of this PPP. Responsibility to lead Vehicle Program Protection working groups and PPP development can be delegated to the Program Protection Lead (PPL). Ultimately, Program Protection is the responsibility of all personnel associated with the Vehicle from the contractors to the end-user.

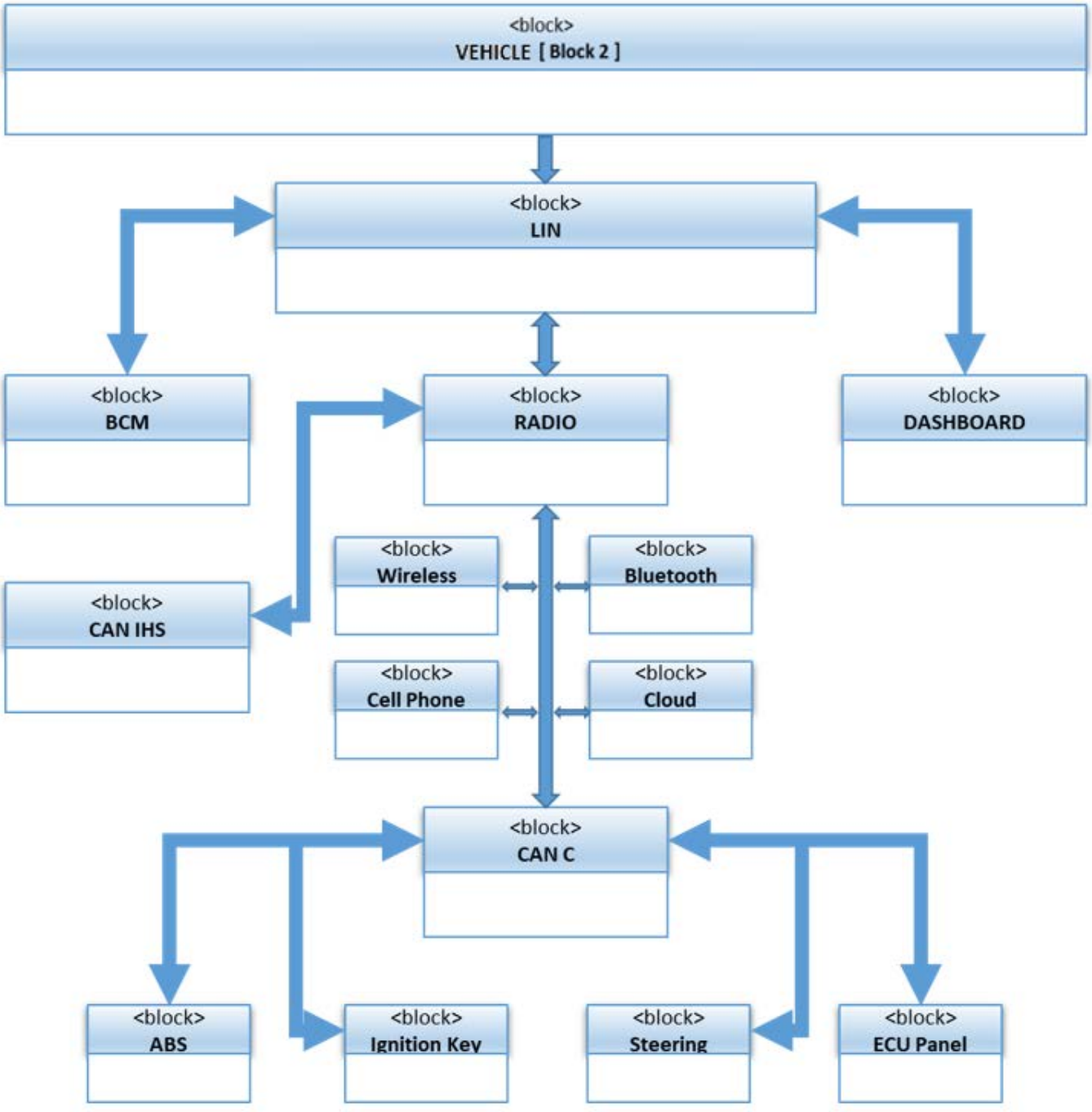


Figure 1.2-1 Systems-Systems Vehicle Network Architecture Viewpoint

Table 1.2-1 identifies the Government parties responsible for various Program Protection efforts for the Vehicle Program.

Table 1.2-1 Program Protection Responsibilities

Title / Role	Name	Location	Contact Information
Program Manager			
Lead Systems Engineer			
Program Protection Lead			
Anti-Tamper Lead			
Information Assurance Lead			
Software Assurance Lead			
SCRM Lead			

In order to translate and apportion the high-level HPT capabilities and constraints into executable and testable requirements, the PM delegates execution responsibility to specific Subject Matter Experts (SME) known as the Systems Security Working Group (SSWG). The SSWG is usually led by the Program Office (PO) Chief Engineer and/or PPL whose responsibility is to guide the Program Protection planning and its implementation throughout the weapon system's life cycle.

Table 1.2-2 illustrates the various SSWG SMEs whose responsibilities are:

- Develop the SSWG Charter
  - Conduct Information Analysis and activities to identify, understand, and protect information about the Program and information residing in the system being acquired
- Evaluate planning and requirements documents
- Generate a SSWG Plan & document the SSWG efforts:
  - Gather all PPP-related information
  - Use existing PPP documentation wherever possible
  - Circulate "Read-Aheads" where practical for the staffing of the PPP
  - Identify inherited CPI and associated PPPs
  - Decompose the system under contract for analysis and testing purposes
  - Generate and maintain SSWG Meeting minutes, charts, etc.
  - Create a historical record of events, decisions, rationale behind the SWWG findings and decisions

[App A Section 1.1.2, High-Performance Team (HPT) implementation of the JCIDS Survivability KPP and Cyber Survivability Attributes (CSAs)]

Table 1.2-2 Systems Security Working Group (SSWG) Membership

Title / Role	Title / Role
Program Manager (PM)	Program Protection Lead (PPL)
Test & Evaluation (Developmental/Operational)	Defense Counterintelligence and Security Agency (DCSA)
Cybersecurity Test Agencies	Authorizing Official (AO)
Logistics	Trusted Systems Network (TSN)
Systems Security Engineering (SSE)	Anti-Tamper Executive Agent (ATEA)
Systems Engineering (SE)	Information Protection (IP)
Intelligence	Counterintelligence

Any questions relating to a particular subject area shall be directed to the respective SME for that discipline. Questions of a general nature can be directed to the Vehicle PPL or the PM.
[WBS 1.1.1, Appoint Personnel to SSWG / appropriate IPT]

2.0 Program Protection Summary

PP/SSE PG Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 2.3.1 A	CDRL 6	-	-	-	-

2.1 Schedule

The current Vehicle program completed Milestone B on February 2015. The system went through Engineering & Manufacturing Development (EMD), as per the Integrated Master Schedule (IMS), as shown by Figure 2.1-1 schedule, and following the Work Breakdown Structure (WBS) for the PP/SSE Guidebook.

Moving into Milestone C, the program successfully evaluated and completed qualification of Block 2, pre-production representative Vehicles in a Low Rate Initial Production (LRIP) quantity of 100. This legacy vehicle is currently in sustainment with an End-of-Life (EOL) support cycle estimated to be between 2040 and 2045. Several modifications to include the Block 2 cyber resiliency upgrades are planned to accommodate vehicular threats, Department of Transportation mandates, parts obsolescence, and end-user suggested requirements.

[App A Section 2.3.1 A, 6]

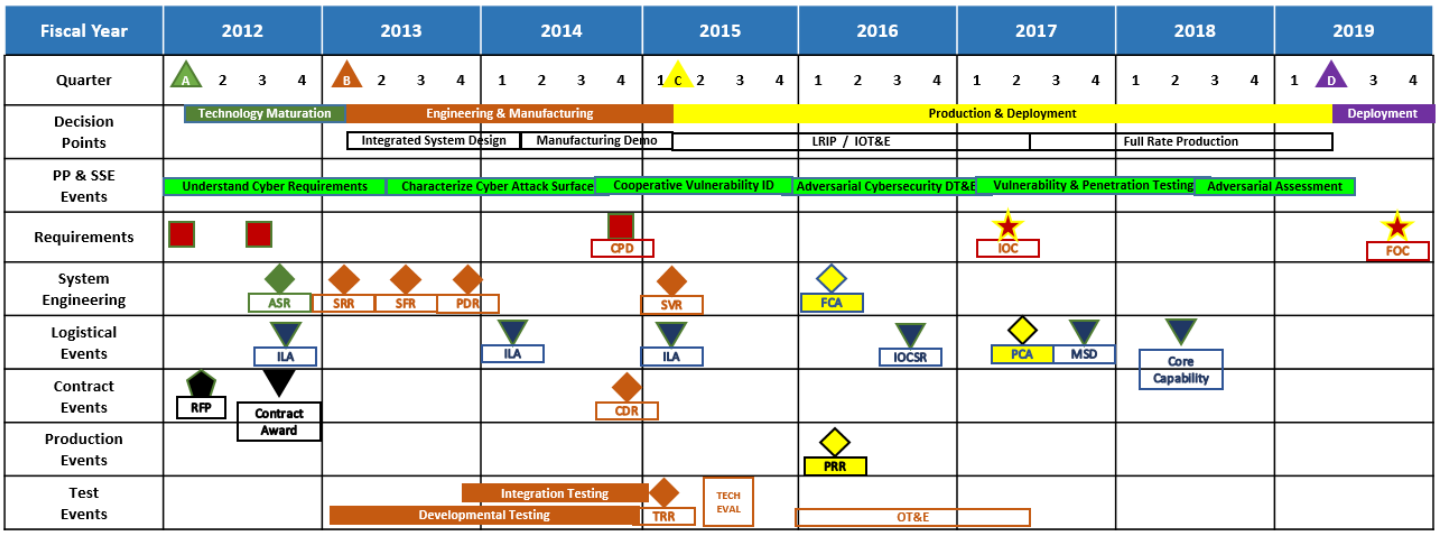


Figure 2.1-1 Vehicle Block 2 Modification Schedule

2.2 CPI, Critical Functions and Components Protection

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 2.3.2 B	CDRL 19	60d < SRR/SFR	60d < PDR	60d < CDR	As Required
Appendix A, 2.3.2 C	CDRL 20	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 2.3.1 C	CDRL 10	60d < SRR/SFR	60d < PDR	60d < CDR	As Required

Table 2.2-1 is a list of vehicle CPI and CCs mapped to the security disciplines of the countermeasures being applied. Blank cells represent countermeasures that are not applied and/or are not applicable to that line item. The PEO validated the current list of CPI and CCs in January 2012 and with further updates on August 2014. The threats and vulnerabilities for which the tabled countermeasures are planned and applied against are documented in subsequent sections of this document.
[App B Section 6.1, Step 2a: Conduct CPI Identification Analysis] [App A Section 2.3.2 C, 19] [App A Section 2.3.2 C, 20]

CPI and Critical Countermeasures Summary

Table 2.2-1, “CPI and CC Countermeasure Summary for Milestone B”, provides the current Vehicle Block 2 program CPI and associated countermeasures. In addition to these countermeasures, the Vehicle PO will apply additional countermeasures inherent to the operation of the Vehicle if it is determined to be appropriate. The Vehicle PO will hold reviews, as needed, to determine any changes to inherited items.

Table 2.2-1 CPI and CC Countermeasure Summary for Milestone B

#	Protected Item (Inherited and Organic)	Countermeasures															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Self-Driving (SD)	X	X	X	X	X	X	I						X			
2	Adaptive Cruise Control (ACC)	X	X	X	X	X	X	I						X			
3	Park Assist System (PAM)	X	X	X	X	X	X	I						X			
4	Lane Departure Warning (LDW+)	X	X	X	X	X	X	I						X			
5	Forward Collision Warning Plus (FCW+)	X	X	X	X	X	X	I						X			

Key	General CMs	Research and Technology Protection CMS	Trusted Systems Design CMs
X = Implemented **I** = Denotes protection already implemented if CPI is inherited.	**1** = Personnel Security **2** = Physical Security **3** = Operations Security **4** = Industrial Security **5** = Training **6** = Information Security **7** = Foreign Disclosure / Agreement	**8** = Transportation Management **9** = Anti-Tamper **10** = Dial-down Functionality	**11** = IA/Network Security **12** = Communication Security **13** = Software Assurance **14** = Supply Chain Risk Management **15** = Systems Security Engineering (SSE) **16** = Other

3.0 Critical Program Information (CPI) and Critical Components

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix B, 7.2	Appendix B: USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 2.3.2 C	Cybersecurity and Trusted Systems and Network	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 2.3.2 C	CDRL 20	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 2.3.1 C	CDRL 10	60d < SRR/SFR	60d < PDR	60d < CDR	As Required

3.1 Identification Methodology

The current threat was defined by the Government Accounting Office (GAO) study GOA-16-350 and report GAO-19-128. Referring to Figure 1.1-2, "Systems-Systems Vehicle Network Architecure Viewpoint", the threat's attack path vector to the vehicle's steering control system is though the CAN-C data bus via the radio system architecture. Any access to the radio system architecture allows the exploitation of the ECUs through multiple probabilistic attack pathway, such as the cell phone or Bluetooth interfaces. From these two paths, a gateway opens to the CAN buses, enabling the ability to send messages from the Vehicle head control unit to every LRU on these interconnected buses.

Using the Functional Thread Analysis (FTA) Report, the SSWG examined the Vehicle missions and functional threads, and then decomposed these functional threads into specific principal system functions. The vehicle's MCFs were determined from these functional threads and their likelihood of contributing to a mission failure, if the function was corrupted or disabled. Mapping these functional threads and functions to the vehicle's modified architecture aided in the identification of the modified vehicle's critical subsystems, Configuration Items (CIs), and sub-components. Special attention was paid to CIs and components containing Information and Communications Technology (ICT).
[App A Section 2.3.2 C, Cybersecurity and Trusted Systems and Network]
[App A Section 2.3.2 C, 20]

After, the SSWG assigned levels of criticality (I, II, III, IV) to the identified CIs and/or vehicle components. The Criticality Analysis (CA) factors or criteria considered were:

- Frequency of a component that was used across multiple functional threads
- The presence of redundancy, expecially for triple redundant system designs and their critical functions
- Subject Matter Expertise (SME) of the design and testing staff, and their supporting contractors

- Any maintenance or servicing support equipment that may have had latent or “back door” defects that could be introduced into the vehicle’s systems
- Critical software applications and modules
- System components that did not directly implement critical functions, but either had unmediated communications access to one or more critical functions or protect a critical function
- System components that were used specifically in the vehicle’s and systems start-up
- System components that were used to establish operational environmental conditions.
- The vehicle’s overall and system architectures to identify “indirect” components, start-up components, and operating environment components
- Any previously identified CC items

Items with assigned criticality levels of I or II were identified as CCs. The SSWG identified the vendors and the Original Equipment Manufacturers (OEM) of these CCs. All other items assessed at levels III and IV were screened to see if they could become CCs. Additionally, the vehicle’s PPL and chief engineer compared the existing criticality levels with the current program’s Minimum Equipment List (MEL) to identify those items that would cause a grave or serious impact during flight.

The Vehicle PO Division leadership met and endorsed the results of these CAs.
[App B Section 7.2, USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components Identification.] [App A Section 2.2.2 C, 20]

CPI Identification and Criticality Analysis Participants

The SSWG re-evaluated the existing CPI and CC derived from the Vehicle Block 1 PPP. As per DoDI 5200.39 and DoDI 5000.022, they were chartered to review the vehicle's current CPI and re-assess them as to their criticality of Low, Moderate and/or High. In order to properly identify CPI, a thorough decomposition of the system was necessary to ensure that all components and subsystems that may contain CPI were evaluated on their own merit. The end result of the system decomposition constituted the items that were evaluated using a CPI Identification Survey and Decision Aid. The DoD Acquisition Security Database (ASDB) was reviewed to ensure Horizontal Protection issues were taken into account. These CPI and their respective CC were found to be similar for Block 1 and Block 2 vehicle designs. IAW DoDI 5200.44, an end-to-end criticality analysis was conducted to identify MCFs and components. It included the identification of any new missions, a decomposition of these mission sets into the functions to perform those missions, and their traceability to the hardware, software, and firmware components that implemented/will implement those functions, protect those functions, or have unmitigated access to those functions. However, in terms of the latest threat and its highly probable attack path vectors, the MCFs and SCFs were changed, as reflected in Table 3.1-1.
[App A Section 2.3.1 C, 10]

Table 3.1-1 MCF/SCF with Initial Risk Assessment

Top Level Functions	Functions	Logic Bearing Components	Priority (Mission vv. Vulnerability)
Mission Critical Functions (MCF)	Transportation (MCF-1)		5
	Entertainment (MCF-2)	Cellular (MCF-2a)	5
		WIFI (MCF-2b)	5
		Radio (MCF-2c)	5
		Blue Tooth Connectivity (MCF-2d)	5
	Self-Driving (MCF-3/CPI-1)	Adaptive Cruise Control (ACC) (MCF-3/CPI-1a)	5
		Park Assist System (PAM) (MCF-3/CPI-1b)	5
		Lane Departure Warning (LDW+) (MCF-3/CPI-1c)	5
		Forward Collision Warning Plus (FCW+) (MCF-3/CPI-1d)	5

Top Level Functions	Functions	Logic Bearing Components	Priority (Mission vv. Vulnerability)
Safety Critical Functions (SCF)	Navigation (SCF-1)	GPS Wireless Modem/WiFi (SCF-1a)	5
	Communication (SCF-2)	Blue Tooth Wireless Modem (SCF-2a)	4
		Cellular Wireless Modem (SCF-2b)	4
	Take-Off / Stop (SCF-3)		5

Timing of Identification and Updates to CPI and Mission Critical Functions and Components

Due to the general non-developmental nature of the Vehicle program, Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) equipment require minimal development through its logistics support and sustainment engineering staff. Discussions of these CCs will be included in internal Technical Interchange Meetings (TIMs) and with supporting contractors for future modifications and upgrades.

CA results mapped down to their CC level were used by the Vehicle's PM and PEO to develop Threat Assessment (TA) Requests (TAR) that were submitted to the Defense Intelligence Agency (DIA) Threat Assessment Center (TAC). DoD contractors are permitted to access the results of these TAs.

If, at any time, DIA TAC reports are not available, the vehicle PO will assume a CIA medium-to-medium-high supplier risk for Level I and selected Level II critical functions and CCs.

The Vehicle PM or their delegate will review the Acquisition Security Database (ASDB) at least once every three (3) years during the PPP review cycle; or more often, if there are changes to the program's CPI or CCs that can affect the Vehicle's PPP.
[App A Section 2.3.1 C, 10]

Process for Identifying CPI and Inherited CPI

The SSWG followed a system decomposition-based process to identify CPI. The process comprised a series of detailed questions from the "*CPI Identification Decision Aid*", Figure A8.1, AFPAM63-113, for each item to ensure that every identified component was considered. These questions included:

- Critical performance requirements
- Comparison to critical technologies subject to import restrictions
- Availability of the technologies on unrestricted domestic markets
- Whether the technology will become obsolete during the anticipated system life cycle
- Review of contractor intellectual property
- Review of contractor manufacturing/development processes or procedures
- Impacts of information compromise
- Potential for system loss or destruction

- Potential for system neutralization or degradation
- Potential for system duplication
- Potential for decreased system effectiveness

For each item, the SSWG considered:

- System capabilities
- Performance parameters
- Mission-related data
- Design data
- Materials
- Manufacturing processes and equipment
- Design methodologies
- Algorithms
- Support and maintenance concepts
- Reliability, maintainability, and availability
- Supply chains
- Training
- Technical data
- Support equipment
- Locations
- Data libraries
- Test and evaluation techniques and locations

They horizontally-leveraged the results of similar security countermeasures for protecting similar technologies used by more than one program or technology projects. This horizontal protection ensures cost-effective application of technology protection efforts and CPI assessments performed for similar platforms and similar systems within those platforms. This CPI assessment was reviewed and approved by the Vehicle PO Division-level leadership.

The Vehicle PO will update the PPP before each Systems Engineering Technical Review (SETR) and use the last update of the phase for the milestone PPP submittals. The System Functional Review (SFR) PPP update will be used as the draft PPP for the Developmental (EMD Phase) RFP. The SSWG supporting the PM will continue to identify any changes in the current inherited and organic CPI, as well as, their related components under DoDI 5200.44 guidance.

Approach for Performing Criticality Analysis

As per DoDI 5200.44, the Vehicle PO shall perform the CA iteratively across the acquisition life cycle of the system/end-product. Its maturity depends on the design phase, updated risks, and current threat and vulnerability data.

This CA might involve SME-generated viewpoints provided during several work sessions (to address system and architecture), as opposed to detailed information collected from numerous program documents. For an early iteration, precision is not possible, as it takes several iterations to complete the initial CA.

Table 3.1-2 details the CA steps to be sequentially followed throughout the iterative CA process for the Vehicle PO, the end result reflected in Table 3.2-1 and Appendix C.

Table 3.1-2 Criticality Analysis Sequence

Identify Missions and Mission-Critical Functions	Sources of Information
1. Identify functional threads and principal system functions. • Derived first during pre-Milestone A and revised as needed for successive development milestones.	Joint Capabilities Integration and Development System (JCIDS) Documents: • Initial Capabilities Documents (ICD) • Capability Development Documents (CDD)
2. If possible or necessary, group the mission capabilities by relative importance. Training or reporting functions may not be as important as core mission capabilities.	Operational Representative Subject Matter Expertise (Integration Experts, Chief Engineers)
3. Identify the system's mission critical functions based on functional threads and the likelihood of mission failure if the function is corrupted or disabled. (Mission critical functions may include navigating, targeting, fire control, etc.).	Activity Diagrams Use Cases Functional Decomposition Potential Department of Defense Architecture Framework (DODAF) Sources • OV-5 (Operational Activity Model) • SV-4 (System Functionality Description) Subject Matter Expertise
Identify Critical Subsystems, Configuration Items, and Components	**Sources of Information**
4. Map the functional threads and functions to the system architecture and identify critical subsystems, Configuration Items (CI), and sub-CIs (components). Note: Focus on CIs and components containing Information and Communications Technologies (ICT). Logic-bearing components have been singled out as often implementing critical functions and as susceptible to life cycle corruption.	System/Segment Design Document Architecture Description Document Requirements Traceability/Verify Matrix Potential DODAF Sources • SV-5a (Operational Activity to System Function Traceability Matrix)
5. Assign levels of criticality (I, II, III, IV) to the identified CIs or components. Factors or criteria may include: • Frequency of component use across functional threads • Presence of redundancy; triple-redundant designs can indicate critical functions.	Subject Matter Expertise • Systems Engineer • Operators Representative • Program Office

Identify Critical Subsystems, Configuration Items, and Components	Sources of Information
6. Identify any CIs or components that do not directly implement critical functions but either have unmediated communications access (i.e., an open access channel) to one or more critical functions or protect a critical function. • Which components give or receive information to/from the critical components? Note: A non-critical component may communicate with a critical function in a way that exposes the critical function to attack. In some cases, the architecture may need to include defensive functions or other countermeasures to protect the critical functions.	Architecture Diagrams Subject Matter Expertise Data Flow Diagram
Initial Start Conditions	**Sources of Information**
7. Identify critical conditions/information required to initialize the system to complete mission-critical functions. • What information is needed to successfully execute capabilities? How is this information obtained, provided, or accessed by the system? • How quickly must information be received to be useful? • Does the sequence in which the system initializes itself (power, software load, etc.) have an impact on performance?	Data Flow Diagram Information Support Plan
8. Based on the answers to the questions above, identify these functions or components to be included in program protection risk management.	
Operating Environment	**Sources of Information**

9. Identify the system functions or components required to support operations in the intended environment. These may include propulsion (the system has to roll, float, fly, etc.); thermal regulation (keep warm in space, keep cool in other places, etc.); or other environmentally relevant subsystems that must be operational before the system can perform its missions	Architecture Diagrams
10. Identify the ICT implementing those system functions and any associated vulnerabilities with the design and implementation of that ICT.	

Critical Suppliers	Sources of Information
11. Identify suppliers of critical configuration items or ICT components	Manufacturing Lead
Note: Repeat this process as the system architecture is refined or modified, such as at Systems Engineering Technical Reviews and major acquisition milestone decision points. • Design changes may result in adding or removing specific CIs and sub-CIs from the list of critical functions and components.	

The expected outcome for the Vehicle Block 2 modification CA is:
- A complete list of MCFs and components
- Criticality level assignments for all items in the list
- Rationale for inclusion or exclusion from the list
- Supplier information for each critical component
- Identification of critical elements for inclusion in a DIA TAC Threat Assessment Center (TAC) Request.

The identification of critical functions, CC and their associated system impacts are addressed in §3.2.

3.2 Inherited CPI and Critical Components

Inherited Items Approach

The Vehicle PO will protect all Vehicle-inherited CPI or CCs at a level commensurate or greater than the requirements of the originating program. The Vehicle PO uses all current equipment with inherited CPI in the manner intended by the originating program office. This equipment has not been altered or otherwise modified to degrade the effectiveness of the countermeasures used to protect that inherited CPI.

In the case of this upgrade for Block 2 vehicles, the Vehicle PO will continue to use any new equipment with inherited CPI in the manner intended by the originating program office. This equipment will not be altered or otherwise modified to degrade the effectiveness of the countermeasures used to protect that inherited CPI for Block 1 vehicles. None of the items identified as CCs were developed and produced specifically for the Vehicle, hence all CCs are inherited CCs.

Inherited CPI and Critical Components Table

Table 3.2-1 Inherited CPI and Critical Components (mandated / example only)

CPI / CC	Inherited Critical Item	Parent Program	Original Use	Planned Use	Variation in CMs	Inherited Program POC
CPI	Adaptive Cruise Control (ACC)	Self-Driving	Radar system	Same	None	U.S. Software System Safety
CPI	Park Assist System (PAM)	Self-Driving	Radar system	Same	None	U.S. Software System Safety
CPI	Lane Departure Warning (LDW+)	Self-Driving	Radar system	Same	None	U.S. Software System Safety
CPI	Forward Collision Warning Plus (FCW+)	Self-Driving	Radar system	Same	None	U.S. Software System Safety

Organic CPI and Critical Components

The Vehicle PO has identified that no Vehicle organic CPI and CCs to exist currently.

Due to the general non-developmental nature of the Vehicle Program, the Vehicle PO acquires COTS and GOTS equipment that require minimal development through Vehicle Contractor Logistical Support (CLS) and Engineering Support Services (ESS) contractors. Therefore, the likelihood of future Organic CPI is minimal. However, discussions of CCs will be included in TIMs for future modifications. The Vehicle PO will perform periodic reviews and in conjunction with these TIMs to determine appropriateness of status, and will provide justification for list inclusion.

4.0 Horizontal Protection

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix B, 5.2	Other Artifacts	30d > ???	60d < PDR	60d < CDR	30d > ???
Appendix B, 6.1	Step 2A : Conduct CPI Identification Analysis	30d > ???	60d < PDR	60d < CDR	30d > ???
Appendix B, 7.1	Conduct CPI Horizontal Consistency Analysis	30d > ???	60d < PDR	60d < CDR	30d > ???

Horizontal protection analysis is the process that determines if critical defense technologies, to include CPI, associated with more than one research, development, or acquisition program, are protected to the same degree by all involved DoD activities (DoDI 5200.39). Horizontal Protection is dependent on the results of the CPI analysis.
Horizontal Protection is necessary to ensure that the Vehicle Block 2 program does not diminish other programs by exposing their similar CPI or its related technology with great risk.

Program Protection Responsibilities

It is the Vehicle's PPL's responsibility for maintaining the Horizontal Protection CPI for the Vehicle Block 2 program. In the event there is a disagreement over Horizontal Protection, the Vehicle PM will initiate discussions with the affected parties to address current CPI countermeasures and the risk of possible loss or compromise, and ensure that the risks are accepted or mitigated by all of the affected parties.

Horizontal Protection Information

The Vehicle Block 2 program has the same Horizontal Protection CPI as the current Block 1 program.
[App B Section 5.2, Other Artifacts] [App B Section 6.1, Step 2A Conduct CPI Identification Analysis]

Alignment and Issue Resolution Protection of Horizontal CPI

In the event there is an issue over Horizontal Protection, the Block 2 program will align its CPI with that of its parent Block 1 program CPI. In cases where the Block 2 CPI are new, they will be evaluated against the Block 1 architecture and CPI for interdependencies and impacts.

Acquisition Security Database (ASDB) Record

The Vehicle Block 2 Vehicle program ASDB shall be updated at each milestone and when a new CPI has been identified by the SSWG. The last ASDB Update was on 8 February 2015 with the next update scheduled for 13 February 2019.

Table 4-1 Horizontal Protection Information

CPI	Other Programs With Same or Similar CPI	Pending Adjudications of CPI? (Y/N)
Adaptive Cruise Control (ACC)	Self-Driving	TBD
Park Assist System (PAM)	Self-Driving	TBD
Lane Departure Warning (LDW+)	Self-Driving	TBD
Forward Collision Warning Plus (FCW+)	Self-Driving	TBD

[App B Section 7.1, Conduct CPI Horizontal Consistency Analysis]

5.0 Threats, Vulnerabilities, and Countermeasures

The CPI Identification Process and Criticality Analysis (CA) provide a foundation for assessing and prioritizing threats to the system, vulnerabilities available to those threats, and countermeasures for mitigating those vulnerabilities. The results of the CA, Vulnerability Assessment (VA), and Threat Assessment (TA) are brought together to perform a risk assessment. The results of the analysis are presented in a risk cube. In the risk cube, the Consequence Factor is determined from the CA levels and the Likelihood Factor is determined from the VA and TA. Possible countermeasures are evaluated to determine if the risk can be lowered to an acceptable level. Possible countermeasures are also constrained by implementation cost. Because threats, vulnerabilities, and countermeasures are constantly evolving, these processes must be applied iteratively throughout the acquisition lifecycle of the system. Details on threats, vulnerabilities, and countermeasures are highlighted in the remainder of this section.

Summary of CPI Threats, Vulnerabilities, and Countermeasures

Table 5.3-1 "*Summary of CPI Threat, Vulnerabilities, and Countermeasures*" based on the results of the CPI analysis, provides the Vehicle Block 2 threats, vulnerabilities and countermeasures to mitigate the resulting AT, cybersecurity, software assurance, SCRM, Systems Security Engineering (SSE), and general security risks to CPI and their critical functions/components. The Vehicle PM conducted an analysis of the system from an adversarial perspective to obtain the information identified in Section 5.1 through Section 5.3 to mitigate resulting risks. Cybersecurity countermeasures are consistent with Table 5.1-1. Supply chain countermeasures are consistent with Section 5.3.4.

5.1 Threats

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 2.3.2 C	Cybersecurity and Trusted Systems and Networks	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 2.3.2 C	CDRL 20	30d > ???	60d < PDR	60d < CDR	-
Appendix A, 2.3.2 E	SCRM				
Appendix A, 1.7	Process Analysis	60d < SRR/SFR	60d < PDR	60d < CDR	As Required
Appendix A, 2.3.2 D	CDRL 21	60d < SRR/SFR	60d < PDR	60d < CDR	As Required

Threat Products POC and Timing

The SSWG have been coordinating the timing and requests for intelligence estimates and threat assessments through the Intelligence and Counterintelligence representatives and their higher echelon counterparts, unnamed in this unclassified document. Using the results of the FTA wherein CCs have been identified, this information is forwarded to the Defense Intelligence Agency (DIA), Threat Assessment Center (DIA-TAC) to produce a Threat Assessment Report related to the medium-and-below risk components associated with the MCFs, SCFs and CPI-associated functions. Also, DIBNet affords sharing of threat information between the SSWG, DoD Intelligence agencies and the Defense Industrial Base (DIB) companies. It is the responsibility of the Vehicle PPL to update, assess and integrate threat information into the PPP whenever a new threat has been identified, annually and as needed. DIA through the SSWG Intelligence members is responsible for supporting intelligence threat products for Level I and Level II CCs based on CA to include critical functions and functions that have unmediated access to critical functions.
[App A Section 2.3.2 C, Cybersecurity and Trusted Systems and Networks]
[App A Section 2.3.2 C, CDRL 20]

Threats of malicious insertion into the development process and tools are considered at all tiers of the development process for critical functions/components. The counterintelligence and intelligence threat products that are the basis for the Vehicle Program's CPI and critical functions/components will be used to identify vulnerabilities and to aiding in the selection of the countermeasures to mitigate risks of compromise. Threat products will be reviewed and/or updated as the threat changes.

Table 5.1-1 Summary of CPI Threat, Vulnerabilities, and Countermeasures

CPI (and supplier) Section 2.0	Threats Section 5.1	Vulnerabilities Section 5.2	Countermeasures
Self-driving	1, 2, 3	4	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.
Adaptive Cruise Control (ACC)	1, 2, 3	4	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.
Park Assist System (PAM)	1, 2, 3	4	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.
Lane Departure Warning (LDW+)	1, 2, 3	4	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.
Forward Collision Warning Plus (FCW+)	1, 2, 3	4	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.

Threat Products Update Frequency

Threat products are tied to specific agency/department release dates and not as special reports for this program.

Threat Products Description and References

When DIA TAC reports are not available, the Vehicle PM will assume a medium to medium-high supplier risk for Level I and selected Level II Critical Functions and Components. Refer to § 5.3.4 for current SCRM risks. **[App A Section 2.3.2 E, SCRM]**

Table 5.1-1 identifies the Vehicle threat products used to identify foreign collection, operational loss and supply chain exploit threats to the program and system. Table 5.1-4 identifies non-specific threats that can be applied to any program.

Specific threats to the Vehicle are found in the Vehicle System Threat Assessment Report (STAR). Please note that the formal threat reports are listed for CPI and TSN. In Table 5.1-1, MDCTA and TTRA are specific to CPI, but the VOLT is a shared report.

Table 5.1-1. Vehicle Threat Product References

Program-Specific Threat Products Used	Classification	Document Date	Organization(s) Producing the Product	Reference to Product
AFOSI Counterintelligence Assessment/Report	S	26 Jan 2015	HQ Office of Special Investigations	AFOSI Counterintelligence Assessment/Report
AFOSI Department of Defense Threat Assessment	S	Dec 2007	Office of Special Investigations	AFOSI Department of Defense Threat Assessment
Capstone Threat Assessment (CTA)	U-S	17 Jul 2017	Defense Intelligence Agency	Capstone Threat Assessment (CTA) Being phased out of the DoD
Foreign Technology Assessment	U	12 Sep 2012	Counterintelligence Service	Foreign Technology Assessment
Integrated Threat Assessment (ITA)	U-S	29 May 2018	Service for Special Assess Programs	Integrated Threat Assessment (ITA)
Multi-Discipline Counterintelligence Threat Assessment (MDCTA)	S/NF	30 Jan 2019	Military Department Counterintelligence Organization	(Not yet completed)
System Threat Assessment Report (STAR)	S	04 Jan 2012	Defense Intelligence Agency	Replaced by the VOLT report
Technology Targeting Risk Assessment (TTRA)	S/NF	01 Jul 2019	Service Intelligence Entities	Authorized users should contact program office for SIPRNet URL
Threat Assessment Remediation Analysis (TARA)	U	Oct 2011	MITRE	Supplement to the VOLT report
Validated Online Lifecycle Threat (VOLT) Report	S	01 Nov 2016	Service Intelligence Production Center	Replacing the STAR report
Radio Module – Bluetooth	U	Oct 2014	Defense Counterintelligence and Security Agency (DCSA)	http://www.ars2000.com/Codenomicon_wp_Fuzzing.pdf
Radio Module – Wi-Fi	U	May 2015	DCSA	http://www.ars2000.com/Codenomicon_wp_Fuzzing.pdf
Technology Collection Trends in the U.S. Defense Industry	U	Oct 2006	Defense Security Service	
Targeting U.S. Technologies	U	Feb 2006	Defense Security Service	

Identified Threats

Table 5.1-4 gives the current threats to the Vehicle Block 1 architecture. These threats are presented at a high-level as any attacks to date have not yielded the perpetrator for further investigation and/or prosecution. The adapted version of the Threat Agent Library (TAL) library specifies 19 different threat agents that are relevant for the automotive industry. Each threat agent is described by nine different attributes. The TAL library provides all the information that is needed in order to determine which threat agents present the greatest risk to the Vehicle. The TAL library is used by security experts while conducting the first two steps of the TARA method. The results of these steps for the Vehicle Block 2 upgrade are given by Table 5.1-2.

A current list of threat agent attributes are:

– Intent describes whether the agent's intent is to cause harm or not

– Access describes what type of access the agent has to the target: internal (insider) or external (no access to internal data or resources)

– Outcome is an attribute that describes the final results of the actions taken by a threat agent that could have business or technical advantage for another competing company by stealing some confidential information

– Resource attribute represents the type of resources the agent has access to (e.g. does the threat agent work alone or in a team with several other threat agents, or it may even have the support of a government implying almost unlimited resources)

– Skills attribute describes the skill level of the agent

– Motivations is a newly introduced attribute that explains the motivation behind an action conducted by each of the threat agents. Whether it is for personal satisfaction or financial gain, it is important to reveal the reason and the intensity behind the attack

A current list of threat agent attributes are (continued):

– Visibility describes the extent to which the agent wants to hide or reveal their identity. Some attacks are known to the victim immediately (overt/covert), while other attacks are hidden (clandestine) so that the victim does not know that an attack even took place

– Limits attribute describes the extent to which the agent would go in order to accomplish their goals. Whether the agent would break the law or not is described by this attribute

– Objective describes the primary action the agent will take in order to achieve their goal

Table 5.1-2 Identified Threats

Threat	Description	Consequence of Threat Realization
Reckless Employee	Non-Hostile Intent. Accidental covert attack.	Lawsuits and Brand Name Damage.
Hacktivist	Hostile Intent. Intentional covert attack.	Copy proprietary code. Ideological motivations.
Organized Crime	Hostile Intent. Intentional covert attack.	Physical Injury and/or Take Control of Vehicle.
Cyber Terrorist	Hostile Intent. Intentional covert attack.	Injure/Destroy/Damage/Take Control of Vehicle. Ideological motivation.
Disgruntled Employee	Hostile Intent. Don't Care if Discovered.	Destroy and/or Damage Vehicle.

Refer to Appendix I for a detailed listing of representative attack path vectors training purposes only.

5.2 Vulnerabilities

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 2.3.1 A	CDRL 2	30d < CDR	60d < PCA	30d > PCA	60d < CI/CSCI
Appendix B, 6.1	Step 2a: Conduct CPI Identification Analysis	30d > ???	60d < PDR	60d < CDR	30d > ???

Potential CPI and Critical Component Vulnerabilities

As cybersecurity vulnerability assessments, DIA TAC assessment, and investigation threat assessments are released, the Vehicle PO will review those that could identify new vulnerabilities for the system in any phase of the acquisition cycle. The PM is responsible for ensuring Vehicle contractors continuously reassess and/or update the Vehicle design to account for the new vulnerabilities. For Milestone B, the anticipated CPI and critical function/component vulnerabilities were based on high-level design and potential vendors. For Milestone C, the specific design, development, supply chain, and CPI and critical function/component potential vulnerabilities have been identified and assessed, as shown in Table 6.1-1, "*Potential CPI and Critical Component Vulnerabilities*".

The specific potential design, development, supply chain, and malicious insertion vulnerabilities may be found in the threat documents listed in Table 5.1-1.

Table 5.2-1 Potential CPI and Critical Component Vulnerabilities

V #	CPI / CC	Identified Vulnerabilities

1	Self-driving	Reverse engineering and discovery of protection measures through characteristics of its software code and its “CAN Bus”
2	Adaptive Cruise Control (ACC)	Reverse engineering and discovery of protection measures through characteristics of its software code and its “CAN Bus”
3	Park Assist System (PAM)	Reverse engineering and discovery of protection measures through characteristics of its software code and its “CAN Bus”
4	Lane Departure Warning (LDW+)	Reverse engineering and discovery of protection measures through characteristics of its software code and its “CAN Bus”
5	Forward Collision Warning Plus (FCW+)	Reverse engineering and discovery of protection measures through characteristics of its software code and its “CAN Bus”

New Vulnerabilities Identification Process

Table 5.2-1 listed vulnerabilities remain the key targets for Hostile and Non-Hostile attacks on the existing Block 1 vehicle architecture.

Vulnerabilities Identification POC and Update Frequency

The Vehicle PPL will be the focal point for all vulnerability updates, as they occur or are reported by intelligence assessments and authorities and/or during their reviews at every milestone, or annually thereafter.

Specify the Frequency that the Vulnerabilities be Re-assessed

Re-assessment of existing vulnerabilities will occur at every milestone and/or as engineering changes to the Vehicle are approved and/or new vulnerabilities are reported by intelligence authoritative sources.

Specify the Way in which Vulnerabilities will be Identified and Mitigated

The Vehicle Uconnect system that allows one to compromise the vehicle steering serves as a roadmap for the mitigation process of future risks, such as for the current Self-Driving threat. The existing vulnerabilities before and after any engineering change or upon receiving a threat assessment will be verified in the Software Integration Laboratory (SIL) within 45 days of their discovery unless SCF-related; where upon, they will be reported within 72 hours of their discovery and/or reporting by an intelligence authoritative source. Once these new vulnerabilities have been verified, they will be documented using the USAF Discrepancy Reporting (DR) system by their Criticality/Severity prioritization, and mitigated by a Tiger Team of developers and test engineers whose final “fix” will be reviewed by the Vehicle SSWG before the PEO’s final approval.

It is USAF policy that if the vulnerability affects a Computer Software Configuration Item (CSCI) that is SCF-related, then the entire CSCI is safety critical.
[App A Section 2.3.1 A, CDRL 2]

The PPL will utilize the USAF Automated Computer Program Identification Number System (ACPINS) for determining the Criticality/Severity level as determined by its Computer Program Identification Number (CPIN) based on its National Security Systems (NSS) MCF impacts to the vehicle.

The means to evaluate the vulnerability will be one of many existing processes such as Structural coverage analysis, safety critical function thread testing, Failure Modes Effects Testing (FMET), etc. If the vulnerability cannot be identified and/or fault-contained, then the risk levels must consider the probabilities of cyber, insider and physical attack path vectors and their impact on the vehicle's SCF and MCF CC.

5.3 Countermeasures

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 1.0	Programmatic Documents	Pre-RFP	BAA	RFP	-
Appendix A, 1.1.1	CSA 04 - Protect System's Information	Pre-RFP	BAA	RFP	-
Appendix A, 1.3	Broad Agency Announcement	Pre-RFP	BAA	RFP	-
Appendix A, 2.3	SOO and SOW	Pre-RFP	30d < PDR	30d < CDR	Quarterly
Appendix A, 2.2	Table 2.2-1	30d > ???	60d < PDR	60d < CDR	30d > ???
Appendix A, 2.3.1 C	CDRL 10	30d > ACA	30d < PDR	30d < CDR	Quarterly
Appendix A, 2.3.3 A	CDRL 30	105d < MS A	60d < PDR	60d < CDR	120d < MS C

Countermeasures have been previously selected and implemented to cover prevention, detection and response, and to mitigate risk to CPI and critical functions/components. These countermeasures are based on the threat and guidance from the DoD AT Executive Agent, "*DoD SCRM Key Practices and Implementation Guide"*, encryption guidance, software assurance techniques (e.g., Common Vulnerabilities and Exposures, Common Attack Pattern Enumeration and Classification, Common Weakness Enumeration, testing), "*National Industrial Security Program Operating Manual* (NISPOM)" guidance, and system security design considerations. Specific Points-Of-Contact (POC) for each countermeasure type are identified in Table 1.2-2.

The Vehicle PO works with contractors for modifications and upgrades to ensure that protection requirements are incorporated in the components selected to satisfy the technical performance requirements for those modifications and upgrades during Technical Interchange Meetings (TIMs). The Vehicle PO discusses the use of trade studies for the implementation of the appropriate countermeasures with the contractors for each CPI item or CC if countermeasures are not considered to adequately protect the item. These trade studies include cost-benefit analyses to ensure that cost effectiveness is included within the trade space.

Contact the Vehicle SSWG for specific information on the implementation characteristics (e.g., prevention, detection, response) for each countermeasure used to protect CPI and critical functions and components.
Table 2.2 1, “CPI and CC Countermeasure Summary for Milestone B”, indicates the planned and actual implementation of the PPP.
Table 5.1-1 addresses the implementation of general countermeasures. Specific countermeasure implementation is addressed in each of the following subsections.
[App B Section 6.1, Step 2a: Conduct CPI Identification Analysis]

Countermeasures Selection Approach

The program had previously performed trade-off analysis to select appropriate countermeasures for the Vehicle Block 1 architecture vulnerabilities.

Countermeasures Implementation Responsibility.

The Chief Engineer and his delegate, usually the PPL, are responsible implementing the countermeasures. The Test Engineer is responsible for validating and verifying that each countermeasure meets its specification control Test Thread/Test Item’s criteria.

Protection Requirements Incorporation into Contracts

The Vehicle PM and Contracts Officer are responsible for the countermeasures incorporated into the contract SOW and its associated DIDs.
[WBS 1.1.1, CSA 04 - Protect System's Information from Exploitation]
[App A Section 1.3, Broad Agency Announcement (BAA), Space and Missile Systems Center (SMC) Recommendations]
[App A Section 2.3, SOO and SOW]

These protection requirements were incorporated into the design and associated contracts as the following protections into the Statement-Of-Work (SOW):

- The contractor shall propose an updated list of CPI based on an assessment of the current and planned Vehicle design and associated subsystems in accordance with DoDI 5200.39, “*CPI Identification and Protection within RDT&E*”
- The contractor shall develop an initial Anti-Tamper (AT) design and associated costs to protect the CPI commensurate with their associated consequence of compromise from hands-on, reverse engineering attacks
- The contractor shall conduct an international market assessment to align with AT&L memo on Defense Exportability Features
- The contractor shall conduct a technical feasibility study that includes costs to remove and/or replace the CPI
- The contractor shall support a TIM with the Program Office and AT Evaluation Team and adjust the AT protections accordingly.
- The contractor shall provide the Initial AT Plan at the Preliminary Design Review (PDR).
- The contractor shall use “blind buys” for all components used to implement Level I critical functions.
- The contractor shall use Defense Microelectronics Activity (DMEA) approved suppliers for all DoD-unique, Application-Specific Integrated Circuits (ASICs).

- The contractor shall conduct a trade study to evaluate the use of ASICs vs. Field-Programmable Gate Arrays (FPGAs) for the long-range tracking function with respect to cost, security, reliability, and performance.
- The contractor shall use secure shipping methods for critical components, including shipments from one supplier to another.
- The contractor shall conduct a trade study to evaluate the cost of using critical function isolation for the track function whether implemented via hardware or software.
- The contractor shall establish secure design and coding standards that are used for all developmental software and verified by static analysis.
- Secure design and coding standards should consider Common Weakness Enumeration (CWE), Software Engineering Institute (SEI) Top 10 secure coding practices and other sources when defining the standards.
- The contractor shall fix those errors detected by static analysis that violate secure design and coding standards.
- The contractor shall use different Original Equipment Manufacturer (OEM) suppliers to implement redundant target discrimination functions.
  [App A Section 1.0, Programmatic Documents]

Countermeasures Implementation Descriptions

Table 5.3-1 provides the Vehicle Block 1 and 2 Countermeasures Descriptions using the existing CSAs from the USAF Weapon System PP/SSE Guidebook, Appendix A, Table 2.2-1.

The Vehicle PO will still adhere to the PEO System Security Guidance memo that addresses countermeasures in general, as well as, SCRM, Software Assurance, Security Detection and Response, and AT.

Table 5.3-1 Countermeasures Implementation Descriptions

CSA ID	System 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 wired and wireless signals to meet mission requirements.
Prevent	**CSA 03 - Secure Transmissions and Communications**
3.1	The system shall encrypt transmissions and communications for data 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 encrypt data at rest (per appropriate classification levels).
4.3	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.
4.4	The system shall employ sanitization processes at the system and subsystem 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 are hardened 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.

CSA ID	System Requirements
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 (Prerequisites CSA 05 and 07)
8.2	The system shall provide capabilities to shed non-mission critical functions, systems/sub-systems, and interfaces (Prerequisites CSA 05 and 07)
8.3	The system shall maintain mission critical functions in a cyber-contested operational environment during/after observed anomaly(ies).
8.4	The system shall maintain safety critical functions in a cyber-contested operational environment during/after observed anomaly(ies) (Prerequisites CSA 04, 05, and 07)
8.5	The system shall fail secure when mission critical functions are no longer operational in a contested environment.
Recover	**CSA-09 - Recover System Capabilities**
9.1	The system shall provide the capability to recover to a known state in near real time.

Countermeasure Implementation Plan vs Actual Tracking

Countermeasures will be selected from the various traditional security disciplines of personnel, industrial, information, and physical security. This includes leveraging the security requirements placed on cleared defense contractors by the National Industrial Security Program (NISP) and DoD Manual 5220.22, National Industrial Security Program Operating Manual (NISPOM). In addition, DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, Risk Management will be used to aid in the selection and implementation of appropriate SCRM key practices.

Refer to the Vehicle SOW and the Defense Federal Acquisition Regulation Supplement (DFARS) clauses listed in the contract for specific details on how the program intends to protect CPI and CCs.

5.3.1 Anti-Tamper (AT)

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
2.3.3 A	CDRL 30	105d < MS A	60d < PDR	60d < CDR	120d < MS C

AT Requirements Identification and Plan Development

Responsibilities

The Vehicle PO is responsible for developing an AT Plan for the Vehicle. The Vehicle parent security office oversees AT policy implementation for all Vehicle programs and will assist the Vehicle PO as necessary in the defining AT requirements for the Vehicle. The Vehicle Security Office will be the liaison with the Air Force

AT lead and Air Force AT Executive Agent.
[App A Section 2.3.3 A, 30]

AT Plan Development Schedule

Refer to AFI 16-110 dtd. 18 September 2018 and AFPAM 63-113 (Section 3.5.4).

5.3.2 Information Assurance

Cybersecurity Countermeasures Adequacy Assessment Responsibility

Cybersecurity for the Vehicle is the responsibility of the Vehicle PO. The Vehicle PM is responsible for ensuring all cybersecurity requirements are identified, incorporated into contracts, and verified and validated.

As Vehicle CPI is identified, the Vehicle PO with support from security office will assess the adequacy of cybersecurity countermeasures with the development of AT measures. Cybersecurity controls will be reviewed in the course of the Cybersecurity Strategy approval process to determine if additional cybersecurity countermeasures are required.

Cybersecurity Schedule

The schedule of key Vehicle pending cybersecurity milestones may be found in Figure 2.1-1.

Implementation of Cybersecurity Protections for DoD Systems Hosting CPI

DoD information systems hosting CPI shall be properly certified and accredited IAW current DoD cybersecurity policy and procedures. Personnel including on-site support contractors who access these systems shall have “need to know” access, and shall receive requisite cybersecurity training IAW security policy, and Vehicle PO cybersecurity policy and instructions. Government entities will comply with DoDI 8582.01 to help minimize the compromise of unclassified DoD information. The Vehicle Cybersecurity Survivability Attributes may be found in Appendix F.

Implementation of Cybersecurity Protections for non-DoD Systems Hosting CPI

Cybersecurity oversight for contractor-owned classified information systems is under the purview of the Defense Counterintelligence and Security Agency (DCSA). The DCSA executes this responsibility as the cognizant security authority for the National Industrial Security Program. Any unique cybersecurity requirements that may arise driven by program peculiarities that exceed standard NISPOM cybersecurity requirements, detailed in NISPOM Chapter 8, “Information System Security”, will be specifically negotiated by Vehicle government program teams in concert with the Vehicle contractors.

Prime contractors will ensure contractual requirements are communicated appropriately to subcontractors involved in each effort. Contractors supporting the Vehicle will identify POCs responsible for maintaining a list of any and all Vehicle Organic and Inherited CPI stored on contractor information systems. These lists will be provided to the Vehicle PPL. Contractors will also comply with Defense Federal Acquisition Regulation Supplement (DFARS) § 252.204.7012, “*Safeguarding Covered Defense Information and Cyber Incident Reporting*”, to help minimize the compromise of unclassified DoD information on contractor information systems. DFARS clause must be disseminated in any subcontracts or similar contractual instruments in which subcontract performance will involve critical defense information or operationally critical

support. The clause must be flowed down without alteration, except to identify the parties, to all sub-tiers handling covered defense information. All Vehicle cybersecurity activities will be executed IAW DoDI 8500.01, *Information Assurance*. The Vehicle Program will follow the Risk Management Framework process IAW DoDI 8510.01, *Risk Management Framework for DoD Information Technology*.

Cybersecurity Controls Negotiations

Any deviations from the cybersecurity protections for non-DoD systems hosting CPI will be controlled by the Vehicle PO contract officer. Contractors may negotiate those controls cost and scope with the Vehicle PO Contract Officer, as needed.

Responsibility for Cybersecurity Controls Flow to Subcontractors

The prime contractor shall flow-down all Specification Controls to the sub-contractors, as in all other requirements under: 48 CFR § 52,219-9, “Small Business Subcontracting Plan”; FAR § 52.212-5(e) or § 52.244-6; and/or DFARS § 252.227-7025 and § 252.219-7003. **[App A Section 1.9 (Para Section 5.3.2)]**

Responsibility for Inventory of CPI Hosted on Contractor Systems

The Vehicle PM shall be responsible for the CPI inventory hosted on the Contractor/Sub-Contractor IT Systems using ACPIN.

Implementation of Cybersecurity Protections for Acquired System Hosting CPI

The contractor/sub-contractor shall be responsible for compliance with NIST 800-171, as per DFARS § 252.204.7012. Only the DoD CIO may grant waivers for a contractor to deviate from NIST 800-171.

5.3.3 Software Assurance

Software Assurance Responsibility

Due to the general non-developmental nature of the Vehicle, Block 2 Program, there is no one in the Vehicle PO who is directly responsible for Software Assurance. The supporting Vehicle Security Office has the current responsibility for implementation of software assurance protections and procedures for all programs. The non-developmental nature of the Vehicle Program severely limits visibility into software development processes of prime and engineering support contractors, and their suppliers. Neither the development nor the design of platform software is conducted by the Vehicle PO; therefore, all software is commercially developed. However, the Vehicle PO ensures the procurement of COTS software meets Federal Vehicle Administration (FVA) requirements for Drive Safety through its contractual requirements.

This scope of organizational responsibility limits the Vehicle PO from accessing/obtaining the following:

- Contractor/supplier software design and testing procedures to ensure protection of the system
- Contractor/supplier secure design inspection and secure coding practices
- Information on contractor/supplier use of software automated static and dynamic analysis tools and code inspections

- Contractor/supplier protection of their software development environments beyond general protections outlined in § 6 of this PPP
- Contractor/supplier source code evaluations for common weaknesses, common vulnerabilities, and common exposures
- Contractor/supplier evaluations for common attack pattern enumeration and classification
- Identification of “software of an unknown pedigree”
- Contractor/supplier use of Software Assurance-based countermeasures; such as, Failover Multiple Supplier Redundancy, Fault Isolation, Least Privilege, System Element Isolation, Input Checking/Validation, and Load Key Countermeasures
- FVA vehicle worthiness requirements; such as, Advisory Circular (AC), support the need for Vehicle contractors and their suppliers to provide software that will be protected in the manner expected above to ensure flight safety.

Software Design and Testing Approach

The Vehicle Software Development Plan (SDP), Version 2.0 reflects the latest design and testing approach for the Block 2 modification with respect to its full-rate production effort.

Application of Software Assurance Countermeasures

Tables 5.3 2 and 5.3.3 are provided as samples of the countermeasures for a software developmental system as used in its architecture, operating environment, design and code with respect to:

- Common Vulnerabilities and Exposures (CVE) - Used to identify and coordinate SW vulnerabilities that enable various types of attacks
- Common Attack Pattern Enumeration and Classification (CAPEC) - Used for the analysis of common destructive attack patterns
- Common Weakness Enumeration (CWE) - Used to examine software architecture/design and source code for weaknesses

The Block 2 modification is a non-developmental effort, hence the sample does not represent the current Vehicle system and contractual effort.

COTS Software and Software of Unknown Pedigree Protection, Testing/Vetting

The existing Vehicle PO developed software uses COTS tools for coding, but its machine-generated code is proprietary. For further discussions, refer to AFPAM 63-113, § 4.8.3.3.

How will the Development Environment be Protected

The Vehicle Block 2 modification is a non-development effort. For further discussions, refer to AFPAM 63-113.

List the Development Environment Tools

The Vehicle Block 2 modification is a non-development effort. For further discussions, refer to AFPAM 63-113.

Development Environment Access

The Vehicle Block 2 modification is a non-development effort. For further discussions, refer to AFPAM 63-113.

Development Environment Access List Management

The Vehicle Block 2 modification is a non-development effort. For further discussions, refer to AFPAM 63-113.

Where will the list be stored, and how often will it be updated?

The Vehicle Block 2 modification is a non-development effort. For further discussions, refer to AFPAM 63-113.

Planned vs. Actual Testing/Evaluation Rates Deviation

The Vehicle Block 2 modification is a non-development effort. For further discussions, refer to AFPAM 63-113.

5.3.4 Supply Chain Risk Management (SCRM)

Supply Chain Risk Management

The Vehicle PO employs several techniques to ensure maximum protection for all parts of the Vehicle. The Vehicle PO, through its program contractors, employs an aggressive review process for diminishing manufacturing sources and material shortage (DMSMS). The Vehicle contractors are responsible for instituting a DMSMS program to minimize and mitigate DMSMS risks. The contractors are responsible for providing a DMSMS report to the Vehicle PO. It is incumbent upon the Vehicle PO to ensure the contractor properly employs a DMSMS program.

In addition, the Vehicle uses a commercially-contracted parts system. This is an FVA-approved parts system that is leveraged to support the broader commercial Vehicles.

Supply Chain Threat Assessments Use and Influence

The contractors are responsible for implementing anti-counterfeiting procedures to reduce risk of installation of counterfeit parts within the Vehicle fleet. It is the responsibility of the contractors to procure material from reputable sources. These techniques provide a sufficient substitute in lieu of standardized trusted supplier and counterfeit protection practices. The contractors are required to have SCRM plans.

The Vehicle Program has limited SCRM procedures. The Vehicle PO relies on its contractors to review purchases of COTS and GOTS hardware and software to minimize the risk of counterfeit hardware components and/or malicious operational software. There is no Government-sponsored developmental environment for the Vehicle Block 2 Program. All Vehicle hardware purchases are COTS and GOTS equipment. Hence, SCRM is incorporated into the Vehicle's risk management process. Unless the Government requires the Vehicle Block 2 contractual design to meet certain hardening requirements, the current baseline vehicle design, development environment and procurement practices will remain commercial- and not military-based processes.

Supply Chain Threat Assessments Use and Influence Responsibility

Sensitive information regarding suppliers and the Vehicle supply chain is handled via the same channels as other sensitive Vehicle information. It is the responsibility of the Vehicle PM and the SSWG Intelligence SMEs to review the current commercial FVA ACs for supply chain threats, and in particular, counterfeit

components and sub-components along with Open Source software used in the machine-generated coding processes of the software developers.

Since the Vehicle platform maintains an FVA type certification, the Vehicle Program also follows FVA circulars related to supplier surveillance and non-conforming parts, including policy for eligibility, quality, and identification of aeronautical replacement parts.

The non-developmental nature of the Vehicle Block 2 Program drives the design and implementation of supply chain processes towards prime and engineering support contractors, and their suppliers. This limits the Vehicle PO from directly accessing/obtaining the following:

- Supply chain sourcing
- Contractor/supplier secure design of supply chain processes
- Contractor/supplier DMSMS risks
- State of the global supply chain for applicable Vehicle components

Supply Chain Threat Assessments Request Timing
Government-related contracts will require compliance with SCRM contract clauses and existing DFARS SCRM mandates, and CDRL-driven reports associated with the vehicle's supply chain posture and risks.

Trusted Suppliers
There are no custom-designed integrated circuits designed and purchased exclusively for the Vehicle Program, including the ACC Upgrade. Custom-designed integrated circuits found in Vehicle hardware, including the Block 2 Upgrade, are the responsibility of the engineering support contractor.

Trusted Fabrication of ASICs.
There are no custom-design based ASICs associated with the Vehicle Block 2 modification.

Utilization of Accredited Trusted Suppliers
The accreditation of Trusted Suppliers will be through the use of the Quality Notes IAW the Vehicle Quality Management Plan (QMP). This White List is proprietary and not for release to the public.

Counterfeit Prevention
Contracts shall include DFARS Subpart 252.246-7007, "Contractor Counterfeit Electronic Part Detection and Avoidance System," and DFARS Subpart 252.239-7018, "Supply Chain Risk."

Table 5.3-2 Application of Software Assurance Countermeasures (sample)

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	100/80	100/80	Yes	75/50
Developmental Critical Function SW	100/80	Two Levels	100/80	100/70	100/80	100/80	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

Table 5.3-3 Application of Software Assurance Countermeasures (mandated / sample only)

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						

5.3.5 System Engineering

Systems Security Engineering Responsibility
Systems Security Engineering (SSE) is the responsibility of the Chief Engineer.

Systems Security Engineering and Systems Engineering Plan
The SSE is tightly integrated with the Systems Engineering process by using the program protection CPI, TSN and Information analyses described in Section 3.1, “Identification Methodology” of this document.

The identified protection requirements are inputs into the SE trade-off analysis that the Systems Engineers use during requirement analysis, architecture, design, implementation, verification and validation phases of EMD. The program protection requirements are integrated into the SE baselines for those protection requirements that are system related. These requirements are part of the Requirements Verification Traceability Matrix (RVTM) which traces each requirement through the design baselines to the verification tests and results.

The protection requirements that affect how the system is built such as secure design and coding standards are incorporated into the SOW as task and constrains on the way the system is designed and built. The progress against these tasks and constraints are presented at each of the SETRs along with the SE baselines.

5.3.6 General Countermeasures
General Countermeasures are provided by Table 5.3-4 that describes general countermeasures common across all USAF platforms.

Table 5.3-4 Vehicle Generic Program Countermeasures/Security Activities

Type	Detail
Communications Security (COMSEC)	Secure telephone or other secure means will be used when classified discussions on CPI are held among the Vehicle PO, contractors, and test facilities. Classified information must be transmitted over secure communications links that utilize NSA-approved components. Sensitive unclassified information must be encrypted using Public Key Infrastructure or other NSA-approved encryption algorithms IAW DoDI 8520.02, DoDI 8523.01, and Air Force Instruction (AFI) 17-1302. Where available, the use of secure voice channels is encouraged. No cell phones, recording devices, or personal digital assistants shall be permitted in areas where classified discussions can be conducted IAW DoDI 8500.01. Management of COMSEC keying material will be implemented IAW Electronic Key Management System 1 and AFI 17-1302.

Type	Detail
OPSEC	OPSEC will be carried out IAW DoD Directive (DoDD) 5205.02, DoD 5205.02-M, and AFI 10-701. **Government Sites:** An OPSEC Plan will be incorporated into each test plan if identified Essential Elements of Friendly Information will be part of the test. The OPSEC coverage extends to all government activities where CPI or other program sensitive information may be exposed, such as program offices and test ranges. **Non-Government Sites:** The contractor shall develop an OPSEC Plan for approval by the Vehicle. No Vehicle information, unclassified (including CPI) or classified information may be supplied, disseminated, discussed, released, provided, transmitted, and briefed, in part or in whole, to any other legal entity, contractor, subcontractor, and vendor not under contract to the Vehicle, except IAW applicable disclosure and release policies and instructions.
Foreign Disclosure/Agreement	All mission sensitive information associated with the Vehicle is restricted for disclosure to foreign nationals.
Education, Awareness and Training	Security education and awareness programs are the most cost-effective security countermeasures. Training is provided to all personnel (military, civilian, and contractor) associated with the Vehicle Program. The PM will institute a training program for newcomers and on a refresher basis. All industry partners who have this PPP, implemented via DD Form 254, "DoD Contract Security Classification Specifications," will implement this training.
Information Security	Marking and classification guidance is contained in the Vehicle Security Classification Guide (SCG). Procedures for marking, handling, control, storage, and transmission of classified material are in accordance with DoDI 5200.01, DoDD 5230.24, DoDD 5230.25, and DoDM 5400.07. Guidance concerning the marking, handling, storage, and transmission of "For Official Use Only" information is prescribed in DoDM 5400.07 and AFI 16-1404. Protections include, but are not limited to: Emissions Security, Two-Person Integrity, Access Controls, Access Listings, Controlled Storage, Background Investigations, Alarms, Security Clearances, Non-Disclosure Agreements, Safes, Need-to-Know, Trusted Computers, and Cryptography. Program contractors will comply with DFARS Clause 252.204-7000, "Disclosure of Information".
Personnel Security	The Vehicle Program implements provisions of DoDI 5200.02, which prescribes the procedures for ensuring appropriate investigative requirements are met, suitability adjudications have been rendered, and the proper level of security clearance has been granted to all Government personnel requiring access to classified materials. In accordance with the provisions of DoDD 5105.42, the Defense Counterintelligence and Security Agency (DCSA) is responsible for ensuring that contractor, Government, civilian, and military personnel are in compliance with established personnel security policies and procedures.
Industrial Security	Contractual requirements for all CPI products or services shall comply with DoD 5220.22-M, the NISPOM, AFI 16-1406, and Air Force Handbook 31-602. CPI in the hands of contractors, subcontractors, and vendors shall be protected as prescribed by the NISPOM, the agency-issued DD Form 254, and this PPP. Enforcement of contractor security requirements is the responsibility of DCSA. DCSA Industrial Security Letter 2016-02 requires contractors to have a written program plan to implement insider threat and cybersecurity requirements.

Type	Detail
Computer Security	Computer security will be carried out in accordance with Air Force Manual 17-1301.
Cybersecurity – Development Environment	Prime contractor network security architecture and configuration will be managed by the Chief Information Officer (CIO) (or equivalent). Network security procedures and countermeasures applicable to subnets containing government Controlled Unclassified Information are available upon request. Program contractors will comply with DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*, and DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting".
Secure System Administration	Networks (Non-classified Internet Protocol Router [NIPR] and Secret Internet Protocol Router [SIPR]) within the enclave are locally managed by the Communications Directorate. Domain controllers and authentication methods are provided by Network operations units. Prime contractor network security architecture, configuration, and authentication controls will be managed by the contractor CIO (or equivalent).
Distribution and Destruction Restrictions and Procedures	Procedures are in place to restrict distribution of sensitive information and properly dispose of critical information and components.
Physical Security	The Vehicle systems is a PL-3 asset as defined by AFI 31-101, and is protected accordingly.
Arms Export and Control Act	Any mission sensitive information associated with the Vehicle is restricted from export to foreign governments.

6.0 Other System Security-Related Plans and Documents

Other System Security-Related Plans and Documents Table

Table 6-1 gives a sample system security documents other than the Vehicle QMP and a Security Plan (SP) had this been a Government contract for procuring the vehicle for military use.

Table 6-1 Other System Security-Related Plans and Documents (mandated) (sample)

Plan	Organization	Link/POC
Counterintelligence Support Plan (CISP)	Service CI	TBD
Test & Evaluation Master Plan	TEMP Approval Authority	TBD
Systems Engineering Plan	SEP Approval Authority	TBD
Software Secure Coding Standards	Contractor SW Design Lead	TBD
Trusted Software Design Techniques	Contractor SW Design Lead	TBD
Secure Software Process Standards	Contractor SW Design Lead	TBD
Foreign Travel Training	Contractor FSO	TBD
Foreign Visit Processes	Contractor FSO	TBD

Key Commitments Table

Presently, there are no Technical Assistance Agreements, Memoranda of Agreement (MOA), Memoranda of Understanding (MOU) or other similar legal vehicles between the contractor and the Government.

7.0 Program Protection Risks

Program Protection Risks Integration

The Vehicle risk management process is documented in USAF PP/SSE Acquisition Guidebook. The guidebook has established a Risk Management Process IAW AFI 63-101/20-101 so that risk management processes are consistently applied across all the programs within the Division. The risk process provides guidance regarding how risk items are identified, analyzed for impacts to the program, reduced or mitigated, and tracked throughout the evolution of the sustainment efforts. The risk process addresses how to report risks, when and where they will be reported, and the metrics to be used for tracking risks.

Risk management is accomplished through the individual weapon system's contracts. The Vehicle PO relies extensively on the contractor's internal risk management processes and practices. The contractor is responsible for flowing this risk management program down to subcontractors, teammates, and vendors. Items that are assessed to be potential risk candidates can be identified by anyone associated with the project (e.g., users, contractors, Vehicle PO personnel).

The Vehicle PM and the appropriate Vehicle modification engineer will ensure risk mitigation efforts are integrated into program plans and schedules as needed across the life of the weapon system to mitigate adverse impacts on achieving weapon system objectives. The Vehicle PO and the contractor periodically review program risks through weekly tag-ups and program management reviews and internally through quarterly Weapon System Reviews. Risk management occurs continuously and iteratively throughout the program life cycle.

Risks may be introduced for program protection-related topics, such as AT, cybersecurity, SCRM, software assurance, and general protection countermeasures as identified in Table 5.3.4. The PPL will be included in risk reviews as necessary to discuss program protection-related risks, and to review overall risks for potential program protection impacts.

When available, the Vehicle PO will use DIA TAC threat assessments to adjust mitigation plans for SCRM risks. In the event a DIA TAC threat assessment indicates a high risk for a supplier of Vehicle components, the Vehicle PO will add a new risk and will manage it using the existing risk processes.

When available, the Vehicle PO will use specific SCRM threat and vulnerability information to adjust mitigation plans for SCRM risks. The Vehicle PO is currently managing one program protection-related risk for SCRM, "Self-Driving," whose Consequence of Compromise (C of C) are shown in Table 7-1.

Residual Risks and Unmitigated Risks Identification.

The program will conduct CPI analysis prior to each SETR with an emphasis on updating the list of CPI to include identifying new CPI, assessing risks to the CPI, and assessing the residual risk that will remain after protection measures implementation.

Table 7-1 Vehicle Program Consequence of Compromise

CPI #	CPI Name	Military Advantage	System Capability	Tech. Adv.	Replace	Class	Cons. (Horiz.)	C of C
1	Self-driving	Low	Unknown	Unknown	Unknown	Secret	Low	Low
2	Adaptive Cruise Control (ACC)	Moderate	Unknown	6 years	Unknown	Secret	N/A	High
3	Park Assist System (PAM)	Moderate	Unknown	6 years	Unknown	Secret	N/A	High
4	Lane Departure Warning (LDW+)	Low	Little Loss	< 3 years	< 3 years	Secret	Low	Low
5	Forward Collision Warning Plus (FCW+)	Low	Unknown	Unknown	Unknown	Classified	N/A	Low

Self-Driving Program Key Drivers

Current PP risk mitigations are based on the “Self-Driving” vulnerabilities and associated CPI and CC reflected in Table 7.2. These pre-Milestone A evaluated elements are still retained in the Block 2 design.

Table 7-2 Self-Driving PP Key Driver Elements

Driver	Known Pre-Milestone A	Data Collection Algorithms	Search Control Algorithms	Track Control Algorithms	GPS	RSC
Consequence of Compromise	Yes	Low	High	High	Low	Low
CPI Sensitivity	Yes	Existence	Sight	Sight	Sight	Sight
CPI Interdependences	Yes	Yes	Yes	Yes	No	Maybe
CPI Locations	Yes	Yes	Yes	Yes	Yes	Yes
Horizontal Protection	Yes	Yes	No	No	Yes	No
Exportability	Some	Yes	Yes	Yes	Yes	Maybe

TSN Analysis

The program will conduct TSN analysis prior to each SETR, with emphasis on updating the list of critical components to include identifying new critical components, assessing risks to the critical components, and assessing the residual risk that will remain after protection measures implementation.

Vehicle Program Threat Assessment (TA) overall Likelihood

The TA impacts to the Vehicle's MCFs are reflected in Table 7-3.

Table 7-3 Vehicle Program TA Overall Likelihood

Function	Threat Assessment (TA) Likelihood	Supply Chain Vulnerability Assessment (VA) Likelihood	Software VA Likelihood	Overall Likelihood
(MCF-1) Transportation	High	High	N/A	Highly Likely (H)
(MCF-2) Entertainment	High	N/A	High	Highly Likely (H)
(MCF-3) Self-Driving	Medium	High	High	Highly Likely (H)

Vehicle Program TA Risk Rating

The TA impacts measured in terms of risk are seen in Table 7-4.

Table 7-4 Vehicle Program TA MCF Risk Ratings

Function	TA Likelihood	Supply Chain VA Likelihood	Overall Likelihood
(MCF-1) Transportation	Level I	VH	VH/H
(MCF-2) Entertainment	Level II	H	H/H
(MCF-3) Self-Driving	Level I	VH	H/H

Vehicle Program Risks Plotted on Risk Before/After Mitigation

The MCF-related risks due to TA impacts are shown in Figure 7-1.

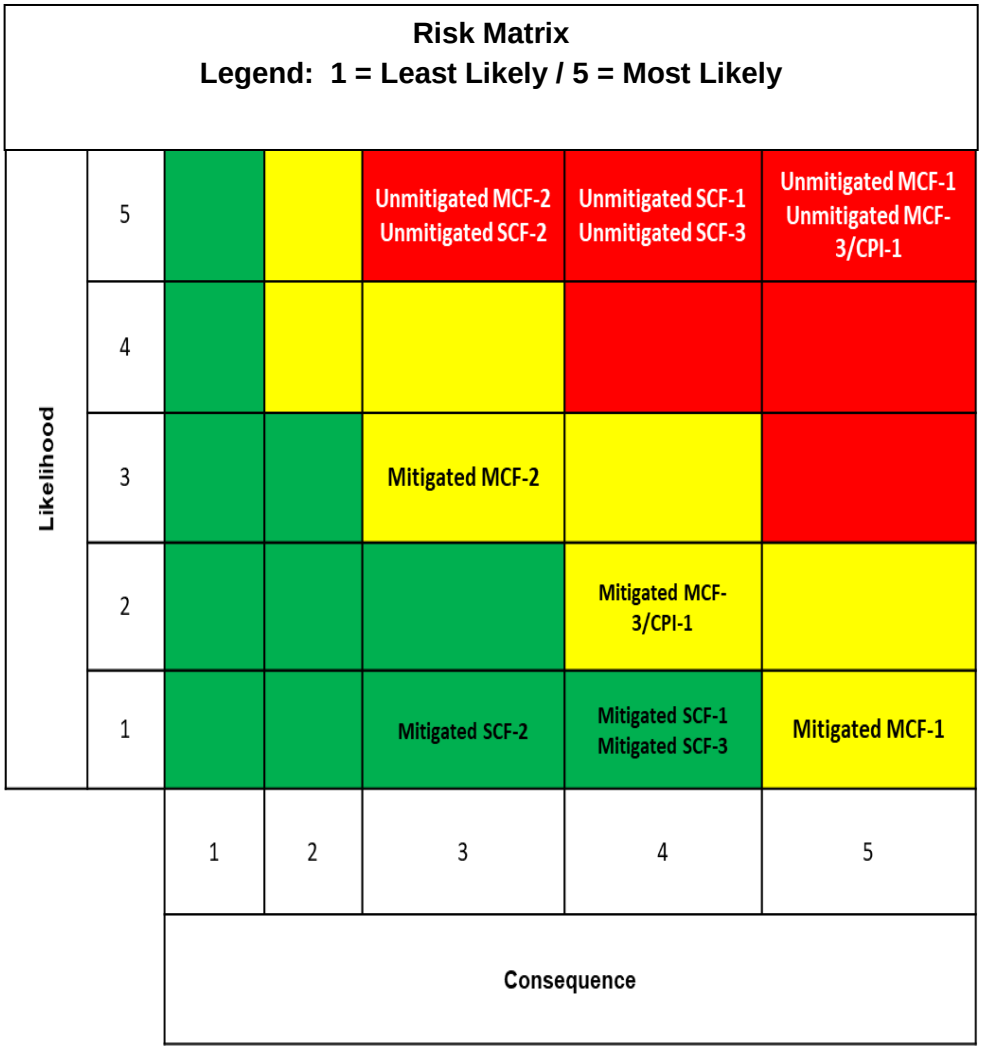


Figure 7-1 Vehicle MCF Risks Mitigated/Unmitigated

8.0 Foreign Involvement

Foreign Involvement Summary

Foreign involvement and defense exportability features specifically relate to CPI and is completely based on CPI analysis results. There are no Foreign Military Sales (FMS) for the Vehicle Block 2 series of vehicles aside from a preliminary design.

There is a potential for future involvement with Canada and Germany. If any foreign sales or co-production activities become formalized, the Block 2 PPWG will be convened to address foreign sales security concerns. Should the program include FMS involvement in the future, a Technology Assessment and Control Plan (TA/CP) will need to be produced and staffed through SAF/IA to identify a systems release determination strategy by the Block 2 PPWG. (An example of a TA/CP is included as a starting point in Annex G.)

- *Summarize any international activities and any plans for, or known, foreign cooperative development or sales of the system.*
- *What are the applicable Technology Security and Foreign Disclosure (TS&FD) processes that will provide guidance to safeguard the sharing of program information with allies and friends?*
- *Have previous generations of this system been sold to foreign allies? Have similar systems been sold?*
- *How will export requirements/restrictions be addressed if a foreign customer/sale is identified? Who is responsible for implementing these requirements?*

Table 8-1 displays a Foreign Involvement Summary format as a sample template only.

Table 8-1 Foreign Involvement Summary (mandated / sample only)

This system is US ONLY (Yes, No, Unknown): Yes				
This system is intended for CONUS deployment only (Yes, No, Unknown): Yes. Not intended for global.				
Approved Disclosures of CPI: None				
Technology Assessment/Control Plan Exists (Y/N/Unknown): No				
Type of Foreign Involvement (IC/FMS/DCS)	**Likelihood of Foreign Involvement (H, M, L)**	**Status (Perceived/Established)**	**Agreements/Licenses in Place (if known)**	**Who is Involved?**
Unknown at this time	L	Perceived	None	TBD

Applicable Technology Security and Foreign Disclosure (TS&FD) Processes

Presently, there are no technology security and foreign disclosure processes in place for the export of the Vehicle Block 2 vehicle.

Previous Sales to Foreign Allies

No previous generations of the present Block 1 baseline vehicle have been sold abroad.

Addressing of Export Requirements/Restrictions and Responsibilities

Any future foreign military sales of the Vehicle shall be IAW the Defense Security Cooperation Agency (DSCA) guidelines while foreign commercial sales will comply with the U.S. Department of Commerce's International Trade Administration. U.S. Commercial Service, Export Administration Regulation (EAR) restrictions and export licensing.

8.1 Defense Exportability Features

Foreign Military Sales and Direct Commercial Sales Potential Risk to Program

As part of the CPI analysis for the Block 2 design in its Milestone A Phase, the expanded exportability entries identified the following exportable options:

- Search Algorithms: Exportable with Limited Capability
- Track Algorithms: Exportable with Limited Capability
- Data Collection Algorithms: Exportable with Limited Capability
- GPS Module: Exportable with Inherited Protections
- Self-Drive Suite Controller: Exportable with Limited Capability

The CPI is being protected at the export level through a trade-off analysis to the balance cost, schedule, and performance of the overall program. The Search algorithms' capability is going to be reviewed by an Export Control Board. There is legacy search code available that does not have the same range and target discrimination capabilities, if the new search algorithms are not exportable.

Defense Exportability Features (DEF) Candidate Viability

DoD's Defense Exportability Features (DEF) initiatives, which include the AT&L DEF Pilot Program and its associated DEF focus area under the Controlling Cost section in Better Buying Power (BBP) 2.0, encourage DoD program management to design and develop technology protection features in systems early in their acquisition life cycle to facilitate earlier foreign sales.

The DEF Pilot Program's primary objectives are to: (1) demonstrate that costs can be reduced and U.S. products can be made available for foreign sales sooner through the incorporation of DEF in initial designs, and (2) garner DEF lessons learned across DoD program experiences to improve the return on investment for future programs.

Presently, no corporate investment into the DEF program is anticipated for the Vehicle.

Hotlink to the Relevant DEF Discussion

Not Applicable (N/A)

Special Access Programs

If the special access program or system contains CPI, the PM will prepare and implement a PPP prior to transitioning to collateral or unclassified status. Security, intelligence, and counterintelligence organizations should assist in developing the PPP. The PPP will be provided to the offices responsible for implementing protection requirements before beginning the transition.

9.0 Processes for Management and Implementation of PPP

Primary responsibility for execution of the PPP during design, development, and test lies with the Vehicle PM with the assistance from the Vehicle PPL and the appropriate SMEs that comprise the SSWG. All Block 2 Vehicle modifications are subject to the appropriate security accreditation processes. Audits and inspections are used to ensure that it complies with applicable cybersecurity and resiliency laws, regulations, and policies. System Engineering Technical Reviews (SETRs) are used to ensure that system security requirements are identified, traced, and sustained throughout the weapon system/end-product acquisition life cycle.

Additionally, the PM designates the PPL as the main program facilitator for the Program Protection Working Group (PPWG). This group represents all functional offices, agencies, and industry including the prime and their sub-contractors, charged with protecting the program from a multitude of security threats. The PPWG make up is determined by the phase of the program and issues being addressed. The PPL determines the make-up of the PPWG prior to each meeting based on issues the PPWG will address.

9.1 Audits/Inspections

Contractual requirements for all CPI products or services shall comply with the NISPOM. CPI in the hands of contractors, subcontractors, and vendors shall be protected as prescribed by the NISPOM, the agency-issued DD Forms 254, and this PPP. The Vehicle PO may authorize assessments of contractors to evaluate the quality and level of commitment to program protection. The Vehicle's Security Office will include protection of CPI in Program Protection Surveys IAW DoDI 5200.39. Prior to any public release of program-related material, the Vehicle PPL will conduct a security and OPSEC review.

9.2 Engineering/Technical Reviews

Addressing of System Security Requirements

Due to the general non-developmental nature of the Vehicle Block 2 Program, the Vehicle PO acquires COTS and GOTS equipment that requires minimal development through its CLS and ESS contractors. The Vehicle PO may tailor the SETR process to incorporate TIMs in lieu of traditional Design Reviews for Vehicle modifications and upgrades to assess the incremental progress of these modifications/upgrades.

PP/SSE, including AT, Software Assurance, SCRM, and Cybersecurity/Resiliency, is an integral part of the Vehicle modification/upgrade process. The Vehicle Chief Engineer is responsible for ensuring the Systems Engineering process addresses system security requirements, and that SSE representatives are adequately represented throughout the Systems Engineering process.

Program Protection Entry/Exit Criteria

The Chief Engineer leads the evaluation of entry and exit criteria to ensure specific SSE requirements and concerns are considered. As new capabilities are introduced to the Vehicle program baseline beyond Block 2, this disciplined modification/upgrade process will be followed to ensure that system security design considerations are adequately addressed.

9.3 Verification and Validation

System Security Requirements Testing Integration

The Vehicle Chief Engineer is responsible for integrating SSE requirements, including CA results, system-level security design trade-offs, supply chain risk and malicious insertion penetration analysis, system security RAs, and Blue or Red team testing into the overall Test and Evaluation (T&E) strategy by updating and identifying these requirements in the Vehicle Test and Evaluation Master Plan (TEMP) and TEMPs for future Vehicle modifications and upgrades.

Vehicle Verification and Validation (V&V) is coordinated through Integrated Test Teams (ITT) chartered for each Vehicle Block upgrade. The PPL is an as-required member of each ITT.

The USAF PP/SSE Weapon System Guidebook in conjunction with the Risk Management Framework (RMF) assessment and authorization process will be followed "…to certify that representative protection, detection, response, and restoration of Cybersecurity controls are properly incorporated into the system."

Link to Relevant Discussion in T&E Documents

Appendix G provides information on the Vehicle Block 2's V&V process.

9.4 Sustainment

Program Protection Requirements and Considerations in Sustainment

IAW Vehicle Life Cycle Management Plan (LCMP), § 8.6, the CCBs may include the appropriate SMEs for the specific Vehicle engineering changes. This change process includes an assessment of each proposed change with regards to technology protection.

Configuration changes that require changes in architecture, introduction of new capabilities, or new component installation will require additional CPI Assessments/CA updates to ensure existing PP countermeasures remain effective throughout the vehicle's life cycle sustainment and to determine if new PP countermeasures are required.

The Vehicle PO will incorporate design analysis, technical reviews, product support element determination, sustaining engineering, operational safety, suitability, and effectiveness into any modification to the Vehicle. Such modification events will drive an analysis of CPI and CCs through such technical reviews and analysis, including discussion of PP-related risks for AT, Software Assurance, SCRM, and Cybersecurity and resiliency. Further, periodic reviews of the platform's CPI and CCs will be conducted throughout the Vehicle's life cycle, taking any technical changes or enhancements into consideration.

Specific demilitarization activities for the Vehicle will follow actions and procedures outlined in the Vehicle disposal/demilitarization Plan, dtd. 4 April 2013. Additionally, demilitarization actions must take into account requirements found in this PPP, the Vehicle Security Classification Guide (SCG), Logistics Support Plans, Technical Orders (TOs), and its technical data and drawings.

Relevant Lifecycle Sustainment Plan (LCSP) language

Refer to Section 15 of the Vehicle LCMP for further guidance.

10.0 Processes for Monitoring and Reporting Compromises

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
Appendix A, 1.6	Cybersecurity Strategy	MS A	Pre-RFP	MS B	MS C , FRP/FD

CPI Compromise/Supply Chain Exploit Response Plan/Procedure

The Vehicle PM will be notified immediately in the event of a CPI compromise or CC compromise to include cyberattacks and/or exfiltration. The circumstances behind the compromise will dictate specific reporting and actions to contain, clean-up, and/or mitigate the concern. Defense Counterintelligence and Security Agency (DCSA) and Air Force Office of Special Investigations (AFOSI) will work with the Facility Security Officer (FSO) for compromises occurring at a cleared contractor facility supporting a military-related contract for the Block 2 modification. Unless circumstances like need-to-know require different actions, supplemental protection measures should be implemented within 72 hours of the initial suspicion and/or report to ensure no further compromises occur. This reporting should comply with OMB Information Collection # 0704-0489, expiration 31 October 2019. After collaborating with the intelligence and counterintelligence communities, the PM will determine if the acquisition strategy needs to be altered. If so, the Vehicle PM may immediately implement additional countermeasures, as appropriate.
[App A Section 1.6, Cybersecurity Strategy]

CPI compromises will also be reported immediately to the appropriate investigation office; in the case of a civil-only compromise, the Federal Bureau of Investigation (FBI), Cyber Division and/or the National Cyber Investigative Joint Task Force (NCIJTF).

Supply chain exploits will also be reported immediately to the Defense Hotline at (800) 424-9098. Incidents specifically involving counterfeit CCs will be reported to the Government Industry Data Exchange Program (GIDEP) following instructions in Appendix D of the Government-Industry Data Exchange Program (GIDEP) Operations Manual. A supply chain exploit occurs when a CC is determined to be a counterfeit, a CC contains malware or is subjected to malicious insertion, or a CC is known to be produced by a threat actor.

An AT event occurs when an item (identified in the AT Plan and protected by AT techniques/ measures) is confirmed to have been compromised either by a threat actor or by other unauthorized persons. AT events are addressed in the Vehicle AT Plan, Appendix D.

The Vehicle PM will notify PMs of Inherited CPI and CCs of incidents involving Inherited CPI and/or CCs.

Anti-Tamper Event or Supply Chain Exploit Definition

A CPI compromise is the attempted and/or communication or physical transfer of CPI to an unauthorized person and/or group, known or suspected exposure of CPI to unauthorized persons, or inadvertent disclosure, alteration, transfer, or physical loss of CPI.

CPI capabilities are Classified and their loss and/or compromise has a substantial effect on the ability of an organization to fulfill its and the system's/end-product's mission. All program personnel privy to CPI should

be aware that unauthorized and/or the inadvertent disclosure of CPI will constitute a loss and/or compromise.

11.0 Program Protection Costs

PP/SSE GB Section	Section Title or CDRL #	Partial Delivery	Partial Delivery	Complete Delivery	Update Delivery
WBS 1.6	Create/Update LCCE & CARD	Pre-MS A	180d < Pre-RFP	45d < MS B	45d < MS C , 45d < FRP/FD

The Vehicle PM has the responsibility to ensure Program Protection costs are estimated and are included in the programs budget and contracts. PP/SSE costs are integrated into the Vehicle Program Block 2 cost estimating and budgeting Service Cost Positions (SCP) processes. Costs are associated with the following categories:

- **Personnel Costs:** Includes the Vehicle government and contractor support labor costs for management and implementation of Vehicle program protection.
- **Product Costs:** Represents funding required for services associated with the development and update of the program protection and supporting plans.
- **Service Costs:** Represents funding required for conducting audits and surveys, training, and related activities.
- **Equipment Costs:** Identifies the funding required for unique material procurement necessary to implement the PPP. These procurements are for items that are not currently available from the existing infrastructure at the various facilities where CPI is located. Costs include software licenses, computers, security containers, etc.
- **Travel Costs:** Includes estimated Vehicle Program government and contractor support costs.
- **Foreign Military Sales Costs:** 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.

11.1 Security Costs

Security Costs above NISPOM Requirements

There are no security costs associated with the Vehicle PP exceeding normal NISPOM costs. Table 11.1-1 is provided as a sample template only.

Table 11.1-1 Security Costs above NISPOM Requirements (mandated/sample only)

Cost Type	Activity	Responsibility	Cost
Personnel Costs:	TBD	Program Manager	$$$
Product Costs:	TBD	Manufacturing, V.P.	$$$
Service Costs:	TBD	Service Manager	$$$
Equipment Costs:	TBD	Operations Manager	$$$
Travel Costs:	TBD	Finance Officer	$$$

Cost Type	Activity	Responsibility	Cost
Ancillary Costs:	TBD	Program Manager	$$$
Total Cost:	TBD	Program Manager	Σ $$$

SCIFs or Other Secure Facilities Construction Requirements

There are no SCIF or other secure facilities construction / MILCON costs associated with the Vehicle PP exceeding normal NISPOM costs.

Limited Access Rosters or Other Similar Instruments Cost

There are no limited access or other similar instrument costs associated with the Vehicle PP exceeding normal NISPOM costs.

11.2 Acquisition and Systems Engineering Protection Costs

There are no separable costs for identifying, incorporating, or verifying program protection requirements. Costs for protecting CPI are inherent in the purchase cost of the units containing Inherited CPI. Costs for protecting CCs are inherent in existing supply chain processes.

Due to reasons identified in Section 5.0, there are no separable costs for software code analyses. Due to reasons identified in Section 5.0, there are no separable costs for anti-counterfeiting measures. The Vehicle PO will evaluate supplier lists as SCRM TAC threat assessments become available.

Acquisition and Systems Engineering Protection Costs Table

Table 11.2-1 is offered as a sample template only.

Table 11.2-1 Acquisition and Systems Engineering Protection Costs (mandated / sample only)

Cost Type	Activity	Responsibility	Cost
Engineering:	Incorporate CA, protection design alternative trade studies and system security requirements into RFP scope	PM	$$$
Engineering:	CA and design alternative trade study	Prime Contractor	$$$
Engineering:	Anti-tamper	Prime contractor	$$$
Engineering:	Trusted Foundry	Supplier	$$$
SCRM:	Evaluate supplier lists	PM, DIA TAC	$$$
V&V:	Software code analysis	PM, Gunter AFB	$$$
V&V:	V&V for anti-tamper architecture	AF AT	$$$
V&V:	Verify satisfaction of system security requirements	PM, verification team	$$$
Sustainment:	Anti-counterfeit measures	Depot	$$$
Total Cost:			$$$

Non-recurring Program Protection Engineering Costs Accounting

Nonrecurring Costs (NCs) are grouped into two categories: “nonrecurring research development test and evaluation costs (RDT&E)” and “nonrecurring production costs.” RDT&E NCs are those costs funded by RDT&E appropriations to develop or improve the product or technology either through contract or in-house DoD effort.

Nonrecurring production costs are those “one-time costs incurred in support of previous production of the model specified and those costs specifically incurred in support of the total projected production run” (DoD Directive [DoDD] 2140.2: “Recoupment of Nonrecurring Costs (NCs) on Sales of U.S. Items). NCs are “sunk costs,” in that the U.S. Government pays them in order to develop or produce a given defense article or weapons system specifically for the U.S. armed forces. NCs may include expenditures for preproduction engineering, special tooling, special test equipment, testing, evaluation, and other related costs.
The Vehicle Block 2 modification has no DoD NC associated with it; but, the Block 2 modification has related NC costs which will be accounted for in the scope of ASC 340-10, which allows for reassessment of the Vehicle historic costs for this effort.

Table 11.2-2 gives the Resolution NRE Metrics and Costs Associated with the Full Rate Production of Block 2 Vehicles. It is provided as a sample-only template.

Table 11.2-2 Resolution NRE Metrics and Costs Associated with the Full Rate Production of Block 2 Vehicles

Resolution Costs	90% Confidence (Lower Limit)	Mean Costs	90% Confidence (Upper Limit)	Weeks to Resolve (Mean)
Reclamation:	$1,000	$20,000	$39,000	12
After Market:	$0	$33,000	$10,000	21
Desktop Solution:	$0	$5,000	$58,000	8
Redesign – COTS:	$82,000	$1,118,000	$2,154,000	42
Redesign – CP:	$542,000	$1,094,000	$1,646,000	61
Redesign – PNHA:	$654,000	$1,010,000	$1,366,000	64
Emulation:	$29,000	$73,000	$117,000	26
Testing:	$35,000	$82,000	$135,000	25
Total Cost:	$167,875	$429375	$690,625	32

Projected Cost-Benefit Tradeoffs Approach in Countermeasure Selection

Ideally, one should have at least two countermeasures for each CC for the purposes of estimating their implementation costs and its risk reduction for each countermeasure (assuming that a countermeasure value of -1 reduces the likelihood by one band in the risk register cube.)

After, determine the residual risk rating for future TSN analyses after the implementation of these countermeasures. Repeated applications of the CA, TA and VA should result in a more refined RA rating and/or identify that another countermeasures may be needed.

For each CC, a certain risk level is assigned. Refer to §5.3, Threat Products POC and Timing for an overview of the countermeasures to be considered for the Cost-Benefit Tradeoff study.

Table 11.2-3, “Cost-Benefit Tradeoff for Countermeasure” is provided as a sample template only.

Table 11.2-3 Cost-Benefit Tradeoff for Countermeasures (mandated / sample only)

Component	Risk Rating	Countermeasures	Cost Impact	Risk Reduction	Residual Risk Rating
Self-driving	1, 2, 3	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.	$30,000	$3,250	$26,750
Adaptive Cruise Control (ACC)	1, 2, 3	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.	$5,000	$1,250	$3,750
Park Assist System (PAM)	1, 2, 3	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.	$25,000	$2,000	$23,000
Lane Departure Warning (LDW+)	1, 2, 3	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.	$2,000	$200	$1,800
Forward Collision Warning Plus (FCW+)	1, 2, 3	The system shall implement safeguards to deter, detect, prevent, and respond to hardware tampering.	$4,000	$400	$3,600

The Cost Impact is a product of the Asset Value on USD in terms of a Single-Loss Expectancy (SLE) and an Annual-Loss Expectancy (ALE) based on their probability of occurrence as a single loss event or a number of loss events over a period of one year. The Risk Reduction Costs are the cost of reducing the risk per single-loss event. The Residual Risk Rating is the result of the percentage of risk tolerance times the inherent risk factor. The resulting score is your risk tolerance or residual risk rating that is expected to remain after the planned response to a risk has been taken.

PPP Appendix A: Security Classification Guide

Information Revealing	Level	Reason	Duration	Remarks
1. Cost information, pricing, or funding pertaining to RDT&E systems	U			
2. Production costs, pricing, or funding related to production quantities and/or options identified in past, current, and future contracts	U/FOUO See remarks			FOIA Exemption 5 applies
3. Production and Delivery Schedules				
a. Planned production quantities	U			
b. Number and delivery schedules for RDT&E and production systems, including options	U			
c. Number and delivery schedules of subsystems and/or major components	U			
d. Data on parts, accessories, and equipment				
(1) Data on parts, accessories, and equipment available in the open market or produced for commercial use	U			

PPP Appendix B: Counterintelligence Support Plan (CISP)

VEHICLE DIVISION

LIFECYCLE MANAGEMENT CENTER (LMC)

AUBURN HILLS MI 48321-8004

NOT RELEASABLE TO FOREIGN NATIONALS

PPP APPENDIX B: COUNTERINTELLIGENCE SUPPORT PLAN (CISP)

Introduction

A formal coordinated report for Counterintelligence (CI) support to protect a weapon system's research and technology. This plan shall address key aspects of the installation, activities, program strategy and the nature of CI activities that are to be employed throughout the program's lifecycle.

Program Managers (PM)

The PM is responsible for the development, coordination and use of the CISP throughout the weapon system's lifecycle. A separate plan may be prepared for each DoD contractor or academic institution where Critical Program Information (CPI) are involved.

Through the use of program documents, DIRs, ISA articles identifying intelligence dependencies and their requirements, AIA or the provided CI Support Activity will provide the identification of intelligence resources and gaps, shortfalls and product delivery timeframes.

The PM shall initiate and coordinate counterintelligence activities supporting the program by following the instructions in DoDI O-5240.24, Enclosure 4. The results of this coordination should be documented in a formal and living plan describing the activities to be conducted by a Defense Counterintelligence Component in support of your program's CI; this plan is known as the Counterintelligence Support Plan (CISP) and is an annex to the PPP.

Request for Information (RFI). Air Force customers will submit an RFI via the appropriate acquisition intelligence unit. The Supporting Intelligence Office (SIO, Attachment 1, and Glossary) attempts to answer the customer's request with existing intelligence. The MAJCOM is the final authority as to whether requirements meet Air Force specifications. If information is available, the customer is provided the information and the RFI is closed. If the customer does not have COLISEUM capabilities, the SIO enters the RFI into COLISEUM and forwards it for the customer. If information is not available, the RFI is forwarded to AF/XOIIA-P, the Air Force Validation Office (AFVO), for validation. Upon validation, the RFI becomes a Production Requirement (PR). The Intelligence Community produces intelligence products, applications, and services based on customer requirements that have been validated in accordance with AFI 14-201 series.

CI Support

Military Department Counterintelligence Organizations (MDCOs) include the Army's 902nd Military Intelligence Group, Navy Criminal Investigative Service (NCIS) and Air Force Office of Special Investigations (AFOSI).

These MDCOs produce Multi-Discipline CI Threat Assessments (MDCITAs), which focus on the foreign collection threat to Critical Program Information (CPI) in Joint and Service ACAT programs and feed into the process for the identification and selection of measures for the protection of CPI. The MDCITA is a key element of the Program Protection Plan (PPP). These MDCOs also address the Targeting Technology Risk Assessment (TTRA), which is another CI threat assessment focusing on CPI and a milestone requirement.

The supporting CI office will compile, combine and disseminate information and conduct of activities to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

The CISP describes the planning for the execution of CI activities for acquisition programs with CPI to include Cleared Defense Contractors considered essential by an acquisition program manager where CPI is present. An acquisition PM could also request, with justification, a CISP for a program that does not identify CPI.

The Defense Counterintelligence and Security Agency (DCSA) coordinates the execution of a DoD Component CISP at cleared defense contractor facilities with CPI, develops and provides training for DoD and defense contractor security personnel regarding CPI protection activities required by (or in) classified contracts and provides unclassified and classified all-source analyses, to include, but not limited to, annual analyses of suspicious contacts and activities occurring with the defense contractor community that could adversely affect the protection of CPI. These reports are disseminated to the defense contractor community and DoD Component heads.

The CI Supporting Activity Compile, combine and disseminate all data to the Program Office and supporting Intelligence Division, and file the related data into the GLADIATOR Acquisition Intelligence database on SIPRNET.

The Initial Response (IR) to a Production Requirements (PR) request is on/about 5 days upon receipt of the PR in the COLISEUM system. A Follow-Up Response (FP) will be sent to the customer within 20 working days of the IR. A Proposed Product Response (PPR) will be transmitted to the customer within 45 working days after the IR. The final product will reflect the agreed to intelligence products, applications and services requested by the customer.

CISP Format

Defense Sector: **Refer to DoDD 3020.40 series, Enclosure 3.**

Defense Sector Lead Agency: **Refer to DoDD 3020.40 series, Enclosure 3.**

Defense Sector Lead Point of Contact (POC): **Your lead for coordinating CI activities and reports.**

DCA Name: **As per the Defense Critical Asset (DCA) List.**

DCA Location: **Full street address and the latitude and longitude of the site containing CI.**

On DoD Installation (Y/N): **Full street address and the latitude and longitude.**

DCA Priority: **Based upon the priority assigned by the Defense Sector Lead in the DCA List.**

DCA POC: **The primary interface with the CI community. Give full contact information including name, address, telephone numbers, and email address.**

Local Enforcement POC: **The first responder to an incident involving a DCA. Should be the closest police department, sheriff's office, fire department, or Military Police. Include organizational name and emergency numbers in 10-digit format.**

Contact Method: **The first responder to an incident involving a DCA. Should be the closest police department, sheriff's office, fire department, or Military Police. Include organizational name and emergency numbers in 10-digit format.**

Joint Worldwide Intelligence Communications Systems (JWICS) ____

SECRET Internet Protocol Router Network (SIPRNET) ____

Secure Telephone Equipment (STE) ____

Unclassified Only ____

CI Lead Agency: **The primary CI element identified in Enclosure 3 to provide CI support.**

Supporting CI Element: **The CI element that either exists on-site or has agreed to cover the asset due to proximity, mission, or other reasons.**

Supporting CI Location: **The identifying data for the principal CI element that provides CI services to the asset. Include organization, address, and telephone numbers.**

Supporting CI POC: **Name of CI agent covering the asset or a DCIP POC at the DoD CI element.**

Other CI Elements (Research and Technology Protection (RTP); Force Protection (FP); Base, Post, or Installation CI Elements): **When an assigned asset has organic CI support or is provided CI support by another DoD Component, the CI Lead Agency shall annotate this coverage in the DCIP CI Coverage Plan. The CI Lead Agency retains responsibility for ensuring CI coverage but can accomplish this through the supporting CI element. For example, the DIB may have an RTP presence with a counterintelligence support plan in place. A military installation will likely have organic CI personnel or someone assigned to provide coverage from another installation. List all known activities.**

Other CI Element Mission: **The main duties performed by the assigned CI element (e.g., RTP, FP, investigations, operations).**

Other CI Element Designator: **Assigned CI Element Designator.**

Other CI Element Location: **Assigned CI Element Location.**

Other CI Element POC: **Name of agent or other method of contacting the CI activity.**

Threat Assessment Type and Date: **List all previous threat assessments created for the asset and the date created.**

CISP Format (continued)

Threat Assessment Produced By (e.g., DoD CIFA, DIA): **Organization(s) that produced the assessment(s).**

Joint Staff Integrated Vulnerability Assessment (JSIVA) Date: **Date of any JSIVAs and identities of the producers, if any.**

Non-DoD Supporting CI Element (e.g. FBI, DHS): **Other agencies that have jurisdiction of the asset such as the FBI, DHS, or Central Intelligence Agency. Repeat this entry if multiple agencies.**

Non-DoD Supporting CI Location: **Identifying data for the CI element that provides CI activities for the critical asset. Include organization name, address, telephone numbers, and email addresses.**

Non-DoD Supporting CI Agency POC: **Name of agent covering the asset or a DCIP POC at the servicing unit.**

Other Defense Sectors Affected: **Due to multiple missions and interdependencies of assets, identify any other Defense Sector that may be affected or related to this asset.**

CISP Review Process

The CISP should be reviewed and updated annually.

PPP Appendix C: Criticality Analysis – Part 1

Top Level Functions	Functions	Supporting Logic-Bearing Components (Include HW/SW/Firmware)	System Impact (I, II, III, IV)
Mission Critical Functions (MCF)	**Transportation (MCF-1)**		
	Entertainment (MCF-2)	Cellular (MCF-2a)	III
		WIFI (MCF-2b)	III
		Radio (MCF-2c)	III
		Blue Tooth Connectivity (MCF-2d)	II
	Self-Driving (MCF-3)	Adaptive Cruise Control (ACC) (MCF-3/CPI-1a)	I
		Park Assist System (PAM) (MCF-3/CPI-1b)	II
		Lane Departure Warning (LDW+) (MCF-3/CPI-1c)	II
		Forward Collision Warning Plus (FCW+) (MCF-3/CPI-1d)	II
Safety Critical Functions (SCF)	**Navigation**	GPS Wireless Modem/WiFi (SCF-1a)	V
	Communication	Blue Tooth Wireless Modem (SCF-2a)	IV
		Cellular Wireless Modem (SCF-3a)	IV

PPP Appendix C: Criticality Analysis – Part 2

Critical Components (Level I/II from Part1)	Missions Supported (#)	Source of Item or Component COTS/GOTS/ Developmental Item	Source of Item or Component Legacy/ New	Integrated Circuit? (Y/N If Y: what kind?)	Specifically Designed for Military Use? (Y/N)	C (L-M-H)	I (L-M-H)	A (L-M-H)
Blue Tooth	MCF-2d	COTS	CAN C Can IHS	No	No	M	H	H
Adaptive Cruise Control (ACC)	MCF-3	COTS	CAN C Can IHS	No	No	M	H	M
Park Assist System (PAM)	MCF-3	COTS	Renesas	Yes v850	No	M	M	M
Lane Departure Warning Plus (LDW+)	MCF-3	COTS	CAN C Can IHS	No	No	N/A	N/A	L
Forward Collision Warning Plus (FCW+)	MCF-3	COTS	CAN C Can IHS	No	No	N/A	N/A	L

PPP Appendix D: Anti-Tamper (AT) Plan

AT Plan (TBD)
Vehicle
Block 2 Upgrade
USAF SAF/AQLS

Undated

VEHICLE DIVISION
LIFECYCLE MANAGEMENT CENTER (LMC)
AUBURN HILLS MI 48321-8004

NOT RELEASABLE TO FOREIGN NATIONALS

PPP Appendix E: Cybersecurity Strategy

Foreward

1. The reuse of existing documentation in preparing the Cybersecurity Strategy document is strongly encouraged where practicable. For example, the integrated schedule in the program's approved Cybersecurity Strategy may be referenced in the "program information" section. However, it is incumbent on the submitting PMO to ensure that any such information is readily available to the document review/approval chain by providing copies of the referenced documents in conjunction with the Acquisition Cybersecurity Strategy document. References to draft documents are not sufficient to support approval of the Cybersecurity Strategy document.

2. In consideration of the different levels of maturity relative to acquisition phases, and to encourage brevity and focus, the following page limitations are imposed:
   - Acquisition Cybersecurity Strategies are not required for Material Development Decisions (MDD)
   - Acquisition Cybersecurity Strategies for Milestone A - 7 pages
   - Acquisition Cybersecurity Strategies for Milestone B or C – 15 pages
   - Acquisition Cybersecurity Strategies for Full Rate Production (FRP) or Full Deployment Decision (FDD) - 15 pages

Tables of content, acronym lists, signature sheets and executive summaries are not required, but if included do not count against the page limitations.

3. As part of the Acquisition Documentation Streamlining effort, DOASD (I&IA) has reached agreement with DASD (SE) proposal that the Acquisition Cybersecurity Strategy be included as an appendix to the Program Protection Plan. This does not affect the current review and approval process for the Acquisition Cybersecurity Strategy document, since only documents that have been approved by the Component CIO and reviewed by the DoD CIO (with a formal review report issued by ODASD (I&IA)/DIAP)) will be appended to the PPP.

4. Program offices should utilize the template on the following page in the preparation of their Acquisition Cybersecurity Strategy documents.

5. Cybersecurity threats must be included in the PPP threat table.

Vehicle Acquisition Cybersecurity Strategy

I. Program and System Description.

A. Program Information ***(Applicable to MS A, B, C, FRP/FDD)***

Identify the Acquisition Category (ACAT) of the program. Identify current acquisition life-cycle phase and next milestone decision. Include a graphic representation of the program's schedule.

B. System Description ***(Applicable to MS A, B, C, FRP/FDD)***

Include or reference a high-level overview of the specific system being acquired. Characterize the system as to type of DoD information system (AIS application, enclave, platform IT interconnection, outsourced IT-based process), or as Platform IT without a GIG interconnection. Include or reference a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together. Describe or reference the system's function, and summarize significant information exchange requirements and interfaces with other IT or systems, as well as primary databases supported. Identify the primary network(s) to which the system will be connected (e.g. NIPRNET, SIPRNET, JWICS, etc.). Include a description or graphic defining the system's accreditation boundary.

II. Cybersecurity Requirements.

A. Sources ***(Applicable to MS A, B, C, FRP/FDD)***

1. Impact Value

Identify the system's impact value as specified in the applicable capabilities document, or as determined by the system User Representative on behalf of the information owner. If the system architecture includes multiple segments with differing impact value combinations, include a table listing all segments and their associated impact value designations, as well as a brief rationale for the segmentation.

2. Baseline Cybersecurity Control Sets

Identify the applicable sets of Baseline Cybersecurity Controls from DoD Instruction 8500.2 that will be implemented. A listing of individual controls is not required.

3. ICD/CDD specified requirements

List any specific Cybersecurity requirements identified in the approved governing capability documents (e.g. Initial Capabilities Document or Capability Development Document).

4. Other requirements

List any Cybersecurity requirements specified by other authority (i.e. Component mandated).

B. Cybersecurity Budget (scope and adequacy) ***(Applicable to MS A, B, C, FRP/FDD)***

Describe how Cybersecurity requirements for the full life cycle of the system (including costs associated with assessment and authorization activities) are included and visible in the overall program budget. Include a statement of the adequacy of the Cybersecurity budget relative to requirements.

III. System Cybersecurity Approach (high level): ***(Applicable to MS B, C, FRP/FDD)***

A. System Cybersecurity technical approach

Describe, at a high level, the cybersecurity technical approach that will secure the system.

B. Protections provided by external system or infrastructure

List any protection to be provided by external systems or infrastructure (i.e. inherited control solutions).

IV. Acquisition of Cybersecurity Capabilities and Support: ***(Applicable to MS B, C, FRP/FDD)***

Describe how the program's contracting/procurement approach is structured to ensure each of the following cybersecurity requirements are included in system performance and technical specifications, RFPs and contracts (as well as other agreements, such as SLAs, MOAs, etc.) early in the acquisition life cycle.

A. System Cybersecurity capabilities (COTS or developmental contract)

B. GFE/GFM (external programs)

C. System Cybersecurity capabilities as services (commercial or government)

D. Information Systems Security Engineering (ISSE) services

E. Cybersecurity professional support services to the program (commercial or government, including A&A support)

Confirm that program contracts/agreements communicate the requirement for personnel performing cybersecurity roles to be trained and appropriately certified in cybersecurity in accordance with DoD Directive 8570.01.

V. System Assessment and Authorization:

A. Process (RMF; DCID 6/3, etc) ***(Applicable to MS A, B, C, FRP/FDD)***

Identify the specific Assessment and Authorization (A&A) process to be employed (e.g., Risk Management Framework (RMF)). If the system being acquired is platform IT without a GIG interconnection, describe any Component level process imposed to allocate and validate cybersecurity requirements prior to operation.

B. Key role assignments ***(Applicable to MS B, C, FRP/FDD)***

Include the name, title, and organization of the Designated Accrediting Authority, Authorizing Official, and User Representative for each separately accreditable system being acquired by the program.

C. A&A timeline ***(Applicable to MS B, C, FRP/FDD)***

Include a timeline graphic depicting the target initiation and completion dates for the A&A process, highlighting the issuance of Interim Authorization to Test (IATT), Interim Authorization to Operate (IATO), and Authorizations to Operate (ATOs). Normally, it is expected that an ATO will be issued prior to operational test and evaluation.

D. A&A approach ***(Applicable to MS B, C, FRP/FDD)***

If the program is pursuing an evolutionary acquisition approach, describe how each increment will be subjected to the assessment and authorization process. If the A&A process has started, identify significant activity completed, and whether an ATO or IATO was issued. If the system being acquired will process, store, or distribute Sensitive Compartmented Information, compliance with Intelligence Community Directive (ICD) 503 "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" is required, and the plan for compliance should Be addressed. Do not include reiterations of the generic descriptions of the A&A process (e.g. general descriptions of the RMF activities from DoDI 8510.01).

VI. Cybersecurity Testing:

A. **Testing Integration** ***(Applicable to MS A, B, C, FRP/FDD)***

Confirm that all cybersecurity testing and A&A activities will be/has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test and Evaluation Strategy and Test and Evaluation Master Plan.

B. **Product Evaluation (e.g. Cybersecurity/Cybersecurity-enabled products)** ***(Applicable to MS B, C, FRP/FDD)***

List any planned incorporation of cybersecurity products/cybersecurity-enabled products into the system being acquired, and address any acquisition or testing impacts stemming from compliance with NSTISSP Number 11.

C. Cryptographic Certification ***(Applicable to MS B, C, FRP/FDD)***

List any planned incorporation of cryptographic items into the system being acquired, and address any acquisition or testing impacts stemming from the associated certification of the items by NSA or NIST prior to connection or incorporation.

VII. **Cybersecurity Shortfalls: (Include as classified annex if appropriate)** ***(Applicable to MS B, C, FRP/FDD)***

A. Significant Cybersecurity shortfalls

Identify any significant cybersecurity shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If applicable, identify any Acquisition Decision Memoranda that cite cybersecurity issues. If no significant issues apply, state "None".

B. Proposed solutions and/or mitigation strategies

If the solution to an identified shortfall lies outside the control of the program office, include a recommendation identifying the organization with the responsibility and authority to address the shortfall.

VIII. Policy and Guidance: ***(Applicable to MS A, B, C, FRP/FDD)***

List the primary policy guidance employed by the program in preparing and executing the Acquisition Cybersecurity Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The DoD Cyber Exchange web site provides an actively maintained list of relevant statutory, Federal/DoD regulatory, and DoD guidance that may be applicable. Capsule descriptions of the issuances are not required.

IX. Point of Contact: ***(Applicable to MS A, B, C, FRP/FDD)***

Include the name and contact information for the program management office individual responsible for the Acquisition Cybersecurity Strategy document. It is recommended that the system's Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.

PPP Appendix F: Cyber Survivability Attributes (CSA)

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

PPP Appendix G: Supply Chain Risk Management (SCRM)

Supply Chain Risk Management
(SCRM)
Plan Outline

01 January 2017

VEHICLE DIVISION
LIFECYCLE MANAGEMENT CENTER (LMC)
AUBURN HILLS MI 48321-8004

NOT RELEASABLE TO FOREIGN NATIONALS

PPP Appendix H: Technology Assessment & Control Plan (TA/CP)

Technology Assessment & Control Plan (TA/CP)

01 April 2019

VEHICLE DIVISION
LIFECYCLE MANAGEMENT CENTER (LMC)
AUBURN HILLS MI 48321-8004

NOT RELEASABLE TO FOREIGN NATIONALS

TABLE OF CONTENTS

SECTION **PAGE**

This ANNEX to the Vehicle Program Protection Plan (PPP) addresses several areas; (1) assessing the feasibility of foreign participation in cooperative programs from a foreign disclosure and technology security perspective; (2) assisting in the preparation of negotiating guidance on the transfer of classified information and critical technologies in the negotiation of international agreements; (3) identifying security arrangements for the program; (4) assisting in drafting the Delegation of Disclosure Authority Letter (DDL) (to be discussed in the next section); (5) supporting the acquisition decision review process; and (6) assisting in making decisions on Direct Commercial Sales (DCS), Foreign Military Sales (FMS), and coproduction or licensed production of the system. This ANNEX requires periodic review. It is produced in accordance with:

AFPAM 63-113, Program Protection Planning

DoDD 5530.3, International Agreements

DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations

DoD 5200.39, Security, Intelligence, and Counter-Intelligence Support to Acquisition Program Protection

John Smith, GS-15

Director
Vehicle Director

H.1.0. PROGRAM CONCEPT

H.1.1. Scope: The program offers access to all aspects of the Vehicle Block 2 program to ***Country X*** for mutual military purposes. It formally designates Country X as an authorized user of (specific capability/airframe offered). In accordance with established DoD policy, prior to becoming an authorized military user of Vehicle Block 2 technology, any foreign nation must conclude a formal agreement with the US DoD covering access to and security of Vehicle Block 2 technology. BRIEFLY DESCRIBE Country X REQUIREMENTS. Where, under previous programs with NATO, some co-development was involved, under this program all program equipment will be procured from the U.S.

H.1.2. Vehicle Block 2 description: (INSERT BRIEF PROGRAM DESCRIPTION HERE)

H.1.3. TA/CP review: This TA/CP and associated Delegation of Disclosure Authority Letter (DDL) will be reviewed, at a minimum, annually and/or as specific technology regarding the Vehicle Block 2 program changes.

The disclosure of classified military information (CMI) must be approved by an appropriate disclosure official. A designated disclosure authority is an official at a subordinate component level that has been designated by the DoD component's principal disclosure authority to control disclosures of classified military information by their respective organization. A Delegation of Disclosure Authority Letter (DDL) is used to delegate disclosure authority to subordinate disclosure authorities. The DDL explains classification levels, categories, scope, and limitations of information under a DoD component’s disclosure jurisdiction that may be disclosed to a foreign recipient. A DDL provides detailed guidance regarding releasability of all elements of a system or technology. The Defense Acquisition Guidebook, Chapter 1, Section 10.5 discusses the role of the DDL in international acquisitions.

The DDL is generated using the guidelines and restrictions identified by the technology assessment and control plan. The DDL’s purpose is to provide disclosure guidance to foreign disclosure personnel so that they may carry out their releasability review functions. Delegated disclosure authorities are responsible for reporting all disclosures of classified information made under their delegation in the Foreign Disclosure System (FDS).

H.2.0. NATURE AND SCOPE

H.2.1. Overview: DESCRIBE FOREIGN COOPERATIVE EFFORT; INCLUDE WHETHER EFFORT IS FMS, DCS, JOINT, INCLUDES SUPPORT FROM COUNTRY X FOR: R&D, PRODUCTION, AND/OR DEPLOYMENT

H.2.2. Countries Participating: The United States and Country X. Detail extent ***of Country X involvement.***

H.2.3. Program Phases: This program covers access to and security and availability of, Vehicle Block 2 military equipment. Acquisition of program user equipment from the US is authorized. The program does not have separate phases Country X may purchase up to X units, at an estimated total value of approximately $XXX million.

INSERT A PROGRAM SCHEDULE; NO REQUIRED FORMAT

H.2.4. Summary of Projected Benefits: With this agreement, Country X is required to provide to the US DoD access to Vehicle Block 2 information, technical data, planning data, test results and reports, program applications, integration designs, differential applications and any additional system improvements as a result of its participation in the Vehicle Block 2 program. Some foreign technology benefit may accrue to the US in OUTLINE HERE (may not apply). Of more importance, however, is the benefit that the US will attain greater military interoperability with Country X during joint exercises and joint operations under wartime conditions. See also H.3.6. for specific details on enhanced U.S./ Country X capabilities through this cooperative effort.

H.2.5. Points of Contact:

M.2.5.1. NAME	OFF/SYM	ORG	PHONE #
M.2.5.2. NAME	OFF/SYM	ORG	PHONE #

H.2.6. Major Milestones: PROGRAM is a continuing program. Milestones for access to PROGRAM are not applicable. INCLUDE HERE “MILESTONES” SUCH AS PROGRAM INITIATION, R&D, FLIGHT TESTING, DELIVERY, SUSTAINMENT, ETC. MAY BE IN CHART FORMAT (SIMILAR TO SCHEDULE ABOVE) OR MERELY A REFERENCE TO THE SCHEDULE

H.3.0. TECHNOLOGY ASSESSMENT

H.3.1. Sensitive Technical Data/Technologies Methodology: The Aspects of Vehicle Program to be protected are described in the following paragraphs. Table 1: *Associated MCTL Technologies*, reflects all Vehicle Program technologies deemed sensitive by the Military Critical Technologies List (MCTL), which COUNTRY X will receive access to and/or knowledge of as a part of this effort. Table 2: *Vehicle Program CPI and CSR*, reflects all Vehicle Program Critical Program Information (CPI) and Critical System Resources (CSR), which COUNTRY X will not have access to or knowledge of.

H.3.2. Vehicle Program Technologies:

INSERT APPLICABLE Vehicle Program SENSITIVE DATA/TECHNOLOGIES … WILL COME FROM MCTL

SECTION	TECHNOLOGY
x.x - EXAMPLE	Definition

Table 1.0: Associated MCTL Technologies

INSERT Vehicle Program CPI LIST…AS FOUND IN ANNEX ?

SECTION	TECHNOLOGY
x.x - EXAMPLE	Definition

Table 2.0: Vehicle Program CPI

H.3.2.1. *Unique design, manufacturing know-how and equipment:* DETAIL WHAT, IF ANY DESIGN, MANUFACTURING KNOW-HOW, OR EQUIPMENT WAS SPECIFICALLY PRODUCED FOR Vehicle Program.

H.3.2.2. *Vehicle Program technological advantage*: LIST WHICH TECHNOLOGIES FROM TABLES 1 AND 2 WOULD GIVE COUNTRY X A MAJOR OPERATIONAL ADVANTAGE

H.3.3. Classification/National Disclosure Policy (NDP) Category: As noted above, access to Vehicle Program requires, as a minimum, release of key material classified CLASSIFICATION. In addition, Vehicle Program technical or operational performance/vulnerability information is classified up to Secret, NDP category 2, may be released to those countries that are approved for access under NDP procedures. For specific details regarding classification of Vehicle Program data, see the Vehicle Program Security Classification Guide (SCG). For access, contact the Vehicle Program security lead at (937) 255-9960.

H.3.4. Comparable Foreign Systems: (INSERT A BRIEF DISCRIPTION OF THE MAJOR FOREIGN COMPETITIVE PROGRAMS APPLICABLE. H.E., RUSSIA HAS SIMILAR UAS TO GLOBAL HAWK CALLED XXXXX.) THIS SECTION HAS NO REQUIRED FORMAT, BUT SHOULD IDENTIFY: COUNTRY, COMPANY, NAME OF COMPARABLE SYSTEM, CURRENT/PROJECTED PERFORMANCE CAPABILITIES, QUALITY, COST, ESTIMATED FIELDING DATES

H.3.5. Active PROGRAM foreign programs: Authorized PROGRAM users to date include: (list countries, for example…NATO, Australia, Germany, etc.) INCLUDE ALSO THE SALE/EXPORT OF SIMILAR OR LIKE TECHNOLOGY/SYSTEMS.

H.3.6. Impact on US/Foreign Military Capability:

H.3.6.1. EXPLAIN HOW/WHY PROGRAM IS UNIQUE, STATE-OF-THE-ART SYSTEM, AND PROVIDE A SUMMARY OF US INVESTMENT, LEVEL OF R&D, ETC.

H.3.6.2. STATE SPECIFIC COUNTRY X CONTRIBUTIONS AND PROGRAM CONTRIBUTIONS TO THE OVERALL ENHANCEMENT OF US MILITARY CAPABILITY AND/OR TECHNOLOGY BASE. INCLUDE A BRIEF DESCRIPTION OF HOW SELLING PROGRAM TO COUNTRY X BENEFITS THE US. The US benefits by increasing interoperability with allies and friendly nations during joint exercises and joint operations under wartime conditions.

H.3.7. Risk of Compromise/Damage: See Table 3.0: *Potential Damage to Vehicle Program if Compromised*. For specific details regarding the following table, refer to the Vehicle Program System Threat Assessment Report (STAR), Vehicle Program Integrated Threat Assessment (ITA), and Vehicle Program Defense Intelligence Agency (DIA) Worldtech Threat Report. Contact Vehicle Program Security Lead at (937) 255-1211 for access to these documents.

Specific Scenarios	Threats	Vulnerabilities	Sub-Systems Affected	Impacts If Exploited
Transfer of a military capability the loss of which would threaten U.S. military effectiveness (i.e. information allowing effective countermeasures to be produced).				
Potential compromise of sensitive information revealing systems' weaknesses that could be exploited to defeat or minimize the effectiveness of U.S. systems.				
Susceptibility to reverse engineering of sensitive design features or fabrication methods				
Extent to which the technology that is to be transferred can be diverted and/or exploited for purposes other than the one intended under the specific program.				
Potential impact of participation on U.S. competitive position or U.S. industrial base, if any.				

Table 3.0: Potential Damage to Vehicle Program if Compromised

NOTE: Be mindful of classification considerations as this Table is populated.

H.3.8. Risk of compromise estimate:

H.3.8.1. **Estimate of Vehicle Program susceptibility:** ***Refer to Vehicle Program threat and vulnerability products including: PPP, STAR, ITA, DIA Worldtech Report, etc***.

H.3.8.2. **Risk posed by Country X:**

H.3.8.2.1. **<u>Country X security apparatus</u>:** ***Country X security practices are XXXX (i.e. on par or better than/adequate/poor) equivalent US security functional areas. There is a (Minimal, Low, Medium, High, Very High) risk of compromise of Vehicle Program technology due to Country X security practices.***

H.3.8.2.2. **<u>Past history of Country X compliance</u>:** ***Insert specific details regarding past history of Country X'S compliance with regards to protection of U.S. information and technology.***

H.4.0. CONTROL PLAN

H.4.1. Release of information: Information to be released will be limited to technical information necessary for installation, operation, test or maintenance of the Vehicle Program equipment and aircraft, not including the cryptographic components. This information is unclassified.

H.4.1.1. DDL: ***This TA/CP, specifically the technology assessment, will be used to develop a (n) Vehicle Program DDL for Country X. This DDL will outline what Vehicle Program information can be released to Country and what Vehicle Program information is not releasable.*** The Vehicle Program DDL is maintained by ASC FDO; ASC/XPD, (937) 255-3131.

H.4.2. Specific restrictions on information/technology release: Foreign nations must procure Vehicle Program information and technology from the US via FMS and specifically account by quantity and application, for all devices procured. Accountability is maintained at the 303 AESW. Foreign nations are not authorized to build the Vehicle Program or to include Vehicle Program technology in any other device or aircraft. Contact the ASC FDO for specific release guidelines.

H.4.2.1. ***Specifically describe what is not to be used released to Country X.***

Examples include: CPI/CSR List, Maintenance Concepts, Exploitation, Anti-Tamper, etc. Coordinate this sub-section with SAF/IA.

H.4.3. Specific restrictions on equipment release: Foreign nations must procure Vehicle Program devices from the US via FMS and specifically account by quantity and application, for all devices procured. Accountability is maintained at the 303 AESW. Foreign nations are not authorized to build the Vehicle Program to include Vehicle Program technology in any other device or aircraft. Contact the ASC FDO for specific release guidelines.

H.4.3.1. Repeat the same information as in Section H.4.2.

H.4.4. Special security procedures: DoD Vehicle Program and all non-DoD entities must follow all rules and regulations regarding the overall security of US information and technology (See Vehicle Program PPP, Appendix A for an exhaustive list of such regulations). Specific protection measures are outlined in detail within Vehicle Program PPP; of particular note, as regards security procedures for ***Country X*** Vehicle Program, are ….. See Vehicle Program PPP for details. For additional insight, contact Vehicle Program Security Lead at (937) 255-1211.

H.4.4.1. **Controls on access of foreign nationals at US facilities supporting Vehicle Program**: ***Outline what procedures or documents exist in the event of FLOs or other visitors to U.S.-based facilities, as a part of this Vehicle Program (e.g. H.E. EVAS, TCPS at contractor locations, procedures for Foreign Visitors…)***

H.4.4.2. **Procedures to control releases by U.S. personnel at foreign facilities:** ***List items such as: Foreign Travel State Department Briefings, ensure travelers do not carry security/technology information on their person. Administer post-travel brief, report any irregularities in travel to appropriate agencies, and further elaboration as needed to cover other agencies within the need-to-know scope of the Vehicle Program.***

H.4.5. Other legal or proprietary limitations on access to and licensed uses of the technology in implementing Technical Assistance Agreements (TAAs): As Applicable.

PPP Appendix I: List of Acronyms

Acronym	Definition
AC	Advisory Circular
ACAT	Acquisition Category
ACC	Air Combat Command
ACPINS	Automated Computer Program Identification and Numbering System
AF	Air Force
AFB	Air Force Base
AFI	Air Force Instruction
AFLCMC	Air Force Life Cycle Management Center
AFOSI	Air Force Office of Special Investigations
AFPAM	Air Force Pamphlet
AM	Amplitude Modulation
AO	Authorizing Official
AOR	Area of Responsibility
AP	Access Point
APT	Advanced Persistent Threat
AR	Aerial Refueling
ASC	Aeronautical Systems Center
ASDB	Acquisition Security Database
ASDB	Acquisition Security Database
ASIC	Application-Specific Integrated Circuit
AT	Anti-Tamper
ATC	Air Traffic Control
ATEA	Anti-Tamper Executive Agent
BBP	Better Buying Power
BCM	Body Control Module
C of C	Consequence of Compromise
CA	Criticality Analysis
CAN	Controller Area Network
CAPEC	Common Attack Pattern Enumeration and Classification
CBR	Capability Based Requirements
CC	Critical Component
CCB	Configuration Control Board
CD	CD
CDD	Capability Development Documents
CDR	Critical Design Review
CF	Critical Functions
CFR	Code of Federal Regulations
CI	Configuration Item
CIO	Chief Information Officer
CISP	Counterintelligence Support Plan
CLS	Contractor Logistic Support

Acronym	Definition
CNS/ATM	Communication, Navigation, Surveillance/Air Traffic Management
COMSEC	Communications Security
CONUS	Contiguous United States
COTS	Commercial Off-the-Shelf
CP	Custom Part
CPI	Critical Program Information
CPIN	Computer Program Identification Number
CSA	Cyber Survivability Attributes
CSAR	Combat Search and Rescue
CSCI	Computer Software Configuration Item
CSRC	Cyber Survivability Risk Category
CTA	Capstone Threat Assessment
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DAG	Defense Acquisition Guidebook
DCS	Direct Customer Sales
DD	Department (of) Defense
DDoS	Distributed Denial-of-Service
DEF	Defense Exportability Features
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DMEA	Defense Microelectronics Activity
DMSMS	Diminishing Manufacturing Sources and Material Shortage
DoD	Department of Defense
DODAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DR	Discrepancy Report
DSCA	Defense Security Cooperation Agency
DSS	Defense Security Service
dtd.	dated
e.g.	for example (exempli gratia)
EAR	Export Administration Regulation
ECU	Engine Control Unit
EGPWS	Enhanced Ground Proximity Warning System
EMD	Engineering & Manufacturing Development
EN	Engineering
EOL	End-Of-Life
ESS	Engineering Support Services
EZS	AFLCMC Technical Engineering Services Directorate, Systems Engineering

Acronym	Definition
FA	Force Application
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FCW+	Forward Collision Warning Plus
FM	Frequency Modulation
FMET	Failure Modes Effects Testing
FMS	Flight Management System
FMS	Foreign Military Sales
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPGA	Field-Programmable Gate Arrays
FSO	Facility Security Officer
FTA	Functional Thread Analysis
FVA	Federal Vehicle Administration
GAO	Government Accounting Office
GIDEP	Government Industry Data Exchange Program
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GS	Global Strike
H	High
HF	High Frequency
HPT	High Performance Team
HQ	Headquarters
HW	Hardware
i.e.	that is (id est)
IAW	In Accordance With
IC	Integrated Circuit
ICD	Interface Control Document
ICT	Information and Communication Technology
IFF	Identification Friend, Foe
IMS	Integrated Master Schedule
IOSS	Interagency Operations Security Support
IP	Internet Protocol
ISO	International Organization for Standardization
ITA	Integrated Threat Assessment
ITT	Integrated Test Team
J/A/C	Joint/Allied/Coalition
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Functional Concept
JIC	Joint Integrating Concept

Acronym	Definition
JOC	Joint Operations Center
KPP	Key Performance Parameter
KSA	Key System Attribute
L	Low
LCMP	Life Cycle Management Plan
LDW+	Lane Departure Warning Plus
LIN	Local Interconnect Network
LoA	Letter of Agreement
LRIP	Low Rate Initial Production
LRU	Local Replaceable Units
M	Medium
MCF	Mission Critical Function
MCO	Major Combat Operations
MDA	Milestone Decision Authority
MDCTA	Multi-Discipline Counterintelligence Threat Assessment
MEL	Minimum Equipment List
MITM	Man-In-The-Middle
MITRE	Mitre Corporation is an American not-for-profit organization based in Bedford, MA
MOA	Memorandum of Agreement
MOU	Memorandum Of Understanding.
N/A	Not Applicable
NAS	Naval Air Station
NASIC	National Air and Space Intelligence Center
NC	Non-recurring Costs
NCIJTF	National Cyber Investigative Joint Task Force
NDI	Network Device Interface
NIPR	Non-classified Internet Protocol Router
NISPOM	National Industrial Security Program Operating Manual
NRE	Non-Recurring Engineering
NSA	National Security Agency
NSS	National Security System
OEM	Original Equipment Manufacturer
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OV	Operational Viewpoint
PAM	Park Assist System
para.	paragraph
PATS	Anti-Theft System
PDR	Preliminary Design Review
PEO	Program Executive Office

Acronym	Definition
PKI	Public Key Infrastructure
PM	Program Manager
PNHA	Peculiar Next Higher Assembly
PO	Program Office
POC	Point of Contact
PPIP	Program Protection Implementation Plan
PPL	Program Protection Lead
PPP	Program Protection Plan
PPWG	Program Protection Working Group
PSTN	Public Switched Telephone Network
QMP	Quality Management Plan
RA	Risk Assessment
RDT&E	Remote Keyless Entry/Start
RNLAF	Royal Netherlands Air Force
RSC	Roll-Over Stability Control
RVTM	Requirements Verification Traceability Matrix
SAE	Society of Automotive Engineers
SAF	Secretary of the Air Force
SCF	Safety Critical Functions
SCG	Security Classification Guide
SCIF	Sensitive Compartmented Information Facility
SCP	Service Cost Positions
SCRM	Supply Chain Risk Management
SD	Strategic Deterrence
SDP	Software Development Plan
SE	System Engineer
SEI	Software Engineering Institute
SEP	Systems Engineering Plan
SETR	System Engineering Technical Reviews
SIL	System Integration Laboratory
SIPR	Secret Internet Protocol Router
SME	Subject Matter Expert
SOO	Statement Of Objectives
SoS	System-of-Systems
SOW	Statement Of Work
SSE	Systems Security Engineering
SSWG	Systems Security Working Group
STAR	System Threat Assessment Report
SUV	Sport Utility Vehicle
SV	System Viewpoint
SW	Software

Acronym	Definition
T&E	Test and Evaluation
TA	Threat Assessment
TA/CP	Technology Assessment/Control Plan
TAC	Threat Assessment Center
TAL	Threat Agent Library
TAR	Threat Assessment Report
TARA	Threat Assessment Remediation Analysis
TBD	To Be Determined
TEMP	Test and Evaluation Master Plan
TIM	Technical Interchange Meeting
TMRR	Technology Maturation and Risk Reduction Phase
TO	Technical Order
TPMS	Tire Pressure Monitoring System
TS&FD	Technology Security and Foreign Disclosure
TSN	Trusted Systems Network
TTRA	Technology Targeting Risk Assessment
U	Unclassified
U.S.	United States
USAF	United States Air Force
USB	Universal Serial Bus
V&V	Verification and Validation
V.P.	Vice President
VA	Vulnerability Assessment
VHF	Very High Frequency
VOLT	Validated Online Lifecycle Threat
WBS	Work Breakdown Structure
WiFi	IEEE 802.11x Series Trademark Networking Technology
WPAFB	Wright Patterson Air Force Base

PPP Appendix J: Representative Attack Path Vectors (For Training Purposes Only)

Attack Path Vector Name	Description
Reverse engineering of lost / stolen / captured components	The adversary disassembles a stolen or captured system to learn technical details about its operation and/or vulnerabilities that may be exploited
Compromise design and/or fabrication of hardware components	APT is able to compromise not merely the distribution, but the design and manufacturing of critical organization hardware at selected suppliers
Adversary intercepts hardware in distribution channel	Adversary intercepts hardware from legitimate suppliers and modifies it or replaces it with faulty hardware
Malicious software update	An attacker uses deceptive methods to cause a user or an automated process to download and install malicious code believed to be valid/authentic
Counterfeit web sites used to distribute malicious software updates	Adversary creates a duplicate of a legitimate web site, which users access and unwittingly download malicious software upgrades, patches, etc.
Components/spares no longer available	Adversaries offer necessary replacement parts, but with malware incorporated
Man-In-The-Middle (MITM) supply chain	Adversary eavesdrops on sessions between organization and external supplier to gain insight into organization's supply chain needs that they can later exploit
Malicious software implantation through 3rd party bundling	The inclusion of insecure 3rd party components in a product or code-base, possibly packaging a malicious component in a product before shipping to customer
Adversary gains unauthorized access by exploiting a software vulnerability	The adversary exploits known or unknown (0-day) software vulnerabilities to bypass security controls and gain unauthorized access
Adversary gains unauthorized access using stolen credentials	The adversary uses stolen user account information or PKI credentials to log into the system
Adversary initiates a botnet attack to disrupt network services	A botnet can be directed to spam a designated target system over a range of ports and protocols, resulting in a Distributed Denial of Service (DDoS) attack
Ex-filtration via removable media	Clandestine transfer of sensitive data to removable media, e.g., printed reports, CD,

Attack Path Vector Name	Description
	thumbdrive, etc., which is physically carried outside the security perimeter
Ex-filtration via external network	Clandestine ex-filtration of sensitive data, encrypted and transferred to a remote system outside the security perimeter using a variety of data formats
Derivation of Critical Program Information from unclassified sources	Aggregation of unclassified and/or unprotected data used to derive sensitive data
Unauthorized / unrestricted copying	Unauthorized copies of sensitive data are made and stored within the security perimeter, for future exfiltration, without document control or accountability
Clandestine changes to software or mission data	Clandestine alteration of software or data so that a system operates in a manner that compromises mission effectiveness or safety
Use of public domain info to identify and target suppliers	Suppliers are targeted for cyber and/or social engineering attack based on adversary's supply chain awareness
Netflow data used to identify critical internal workflows	Adversary analyzes netflow traffic data to identify and target key network workflows, IT resources, and/or personnel
Shell company established to export critical technologies	Adversary sets up a dummy company for the purpose of acquiring products that contain restricted or export-controlled technologies for shipment overseas
Software defects hidden/obscured by code complexity	Highly complex code can obscure software defects, even by static source code analysis tools
Use of counterfeit parts of foreign or unknown origin	Insertion of counterfeit parts of foreign origin into products destined for the U.S. having potential to degrade or sabotage performance and reliability of systems
Hardware/Software baseline manipulations	An adversary in the employ of a solution provider subverts computers and networks through subtle hardware or software manipulations
Hiding backdoors and features for unauthorized remote access	An adversary in the employ of a software supplier deliberately hides backdoors and features for unauthorized remote access and use
Foreign hardware incorporated into computing environment	Hardware incorporated into the computing environment that was manufactured overseas or acquired from a foreign-owned domestically controlled company
Foreign software incorporated into computing environment	Software incorporated into the computing environment that was developed overseas or

Attack Path Vector Name	Description
	acquired from a foreign-owned domestically controlled company
Malicious code pre-installed	Malicious code (e.g., viruses, logic bombs, self-modifying code, spyware, trojans) is pre-installed on components being integrated into the computing environment
Disruption of critical product or service	Failure or disruption in the production or distribution of a critical product or service
Malicious or unqualified service provider	Reliance upon a malicious or unqualified service-provider for the performance of technical services
Installation of unintentional vulnerabilities	Installation of hardware or software that contains unintentional vulnerabilities
Zero-day vulnerabilities	Vulnerabilities exist in new or updated software, including operating systems, for which patches or fixes do not yet exist
Misconfigured file system access	Discretionary access for users to system and user folders and files has been set in a manner inconsistent with access/permissions policies and intent
Compromised network server	A compromised server is used to attack client systems requesting network services, execution environments, or access to data
E-mail attachment	Means by which malicious code can be introduced into a system and potentially be capable of system compromise including data exfiltration
Password misuse	Password sharing, a form of password misuse, can lead to unaccountability with respect to execution of software based critical mission functions
Data or information leakage	Social networking sites are used by attackers to gather sensitive information about an organization, its employees, work programs, and technologies used
Auditing circumvention	Preventing a system administrator from starting an audit process could allow an adversary to carry out an attack without possible indicators being recorded
DNS spoofing (cache poisoning)	Results in rerouting a request for a web page, causing the name server to return an incorrect IP address, diverting traffic to another computer, often the attacker's
Use of open source software	Introduction of malicious code into software through insertion of malicious code into open source libraries
Malicious code insertion: Software development – requirements analysis phase	Hidden in software’s requirements

Attack Path Vector Name	Description
Malicious code insertion: Software development – design phase	Hidden in software's design
Malicious code insertion: Software development – implementation phase	Appended to legitimate software code Added to linked library functions Added to installation programs, plug-ins, device drivers, or other support programs Integrated into development tools (e.g., compiler generates malicious code)
Malicious code insertion: Software development – testing phase	Inserted via tools during system test

APPENDIX F – SSE Requirements Implementation Assessment

1 SSE Requirements Implementation Assessment.

1.1 Introduction.

During the design and development of a new weapon system, or modification to an existing weapon system, an assessment of how well cybersecurity and 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 F-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 46 (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.

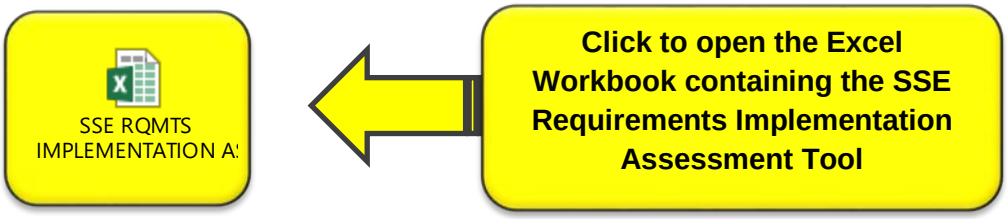


TABLE F-1: Timeline of SSE Requirements Implementation Assessment

USAF Weapon System PP/SSE Guidebook - WBS Step	WBS Step Description	Action	Tool
1.3.6.1	Initial Requirements Development	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. See Figure F-1. This is only required for the initial assessment. All updated assessments require only assessing the modification independently.

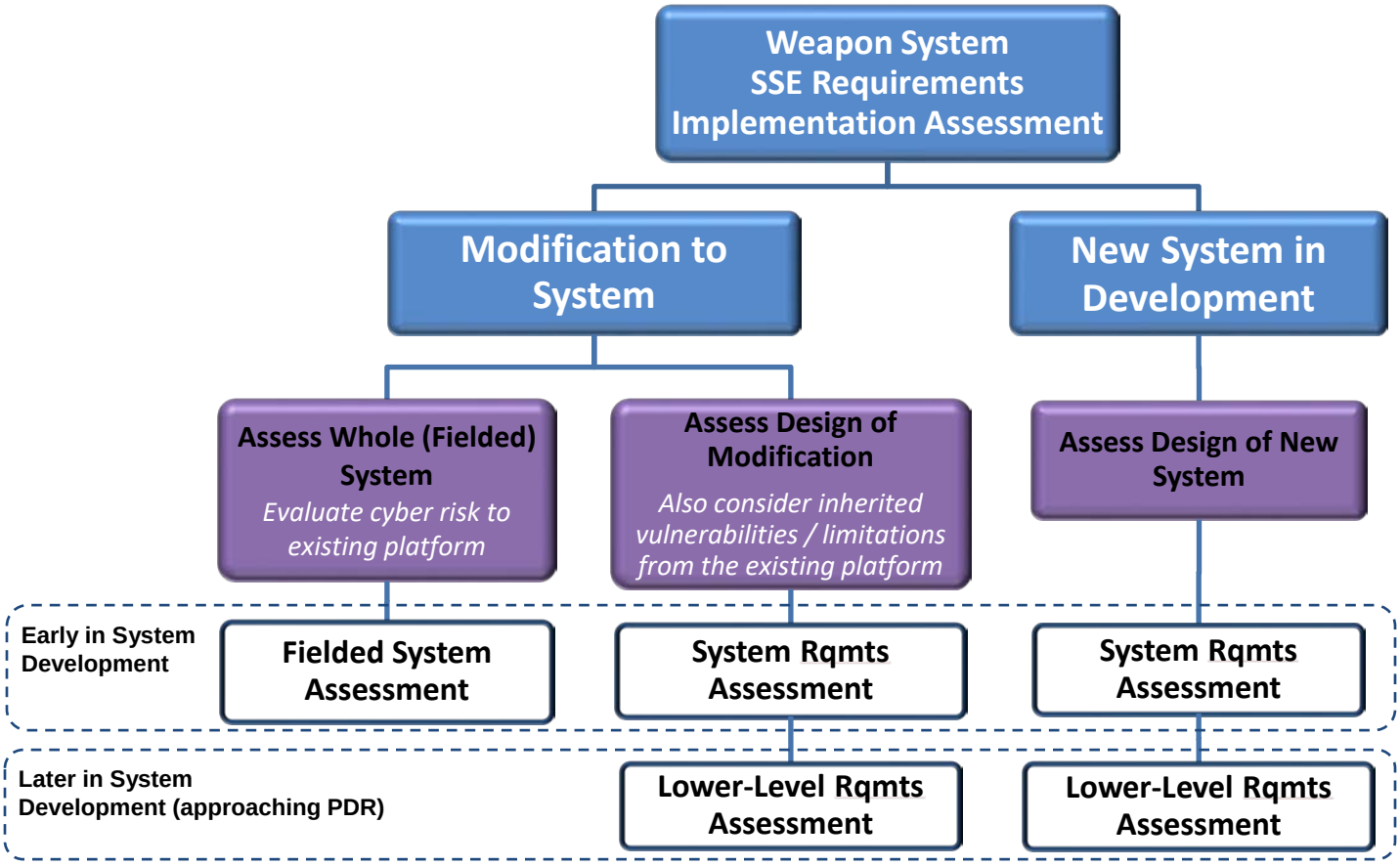


FIGURE F-1: SSE Requirements Implementation Assessment.

1.2.2 Modification to an Existing Weapon System.

For a system modification, first assess the existing weapon system platform, and then assess the modification design. Both of these assessments will use the SSE requirements within this guidebook (Appendix A: SSE Acquisition Guidebook, Attachment 1) as the basis for evaluation, although the methodology will be slightly different.

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 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 resiliency requirements

for the modification. For example, there may be existing cyber vulnerabilities in the 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 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.

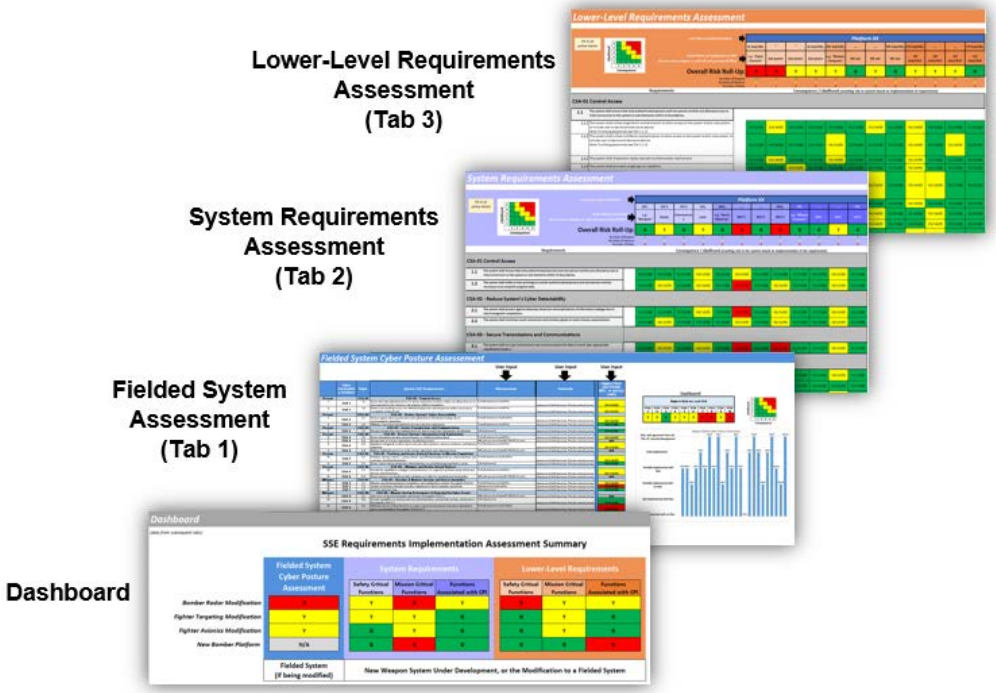


FIGURE F-2: SSE Requirements Implementation Assessment Tool.

1.2.3 New System Development.

For assessing a new 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.

APPENDIX G – Relationship to Other Processes

1.0 Relationship to Other Processes.

In addition to the standard acquisition life cycle, the PP/SSE process is related to the Risk Management Framework, as well as cybersecurity test and evaluation (specifically the Mission Based Cyber Risk Assessment).

1.1 PP/SSE Process and RMF.

Figure G-1 shows the RMS process. While Figure G-2 shows the PP/SSE process. On Figure G-2, the yellow boxes overlaid on the process illustrate the overarching areas where RMF activities are taking place during the PP/SSE process.

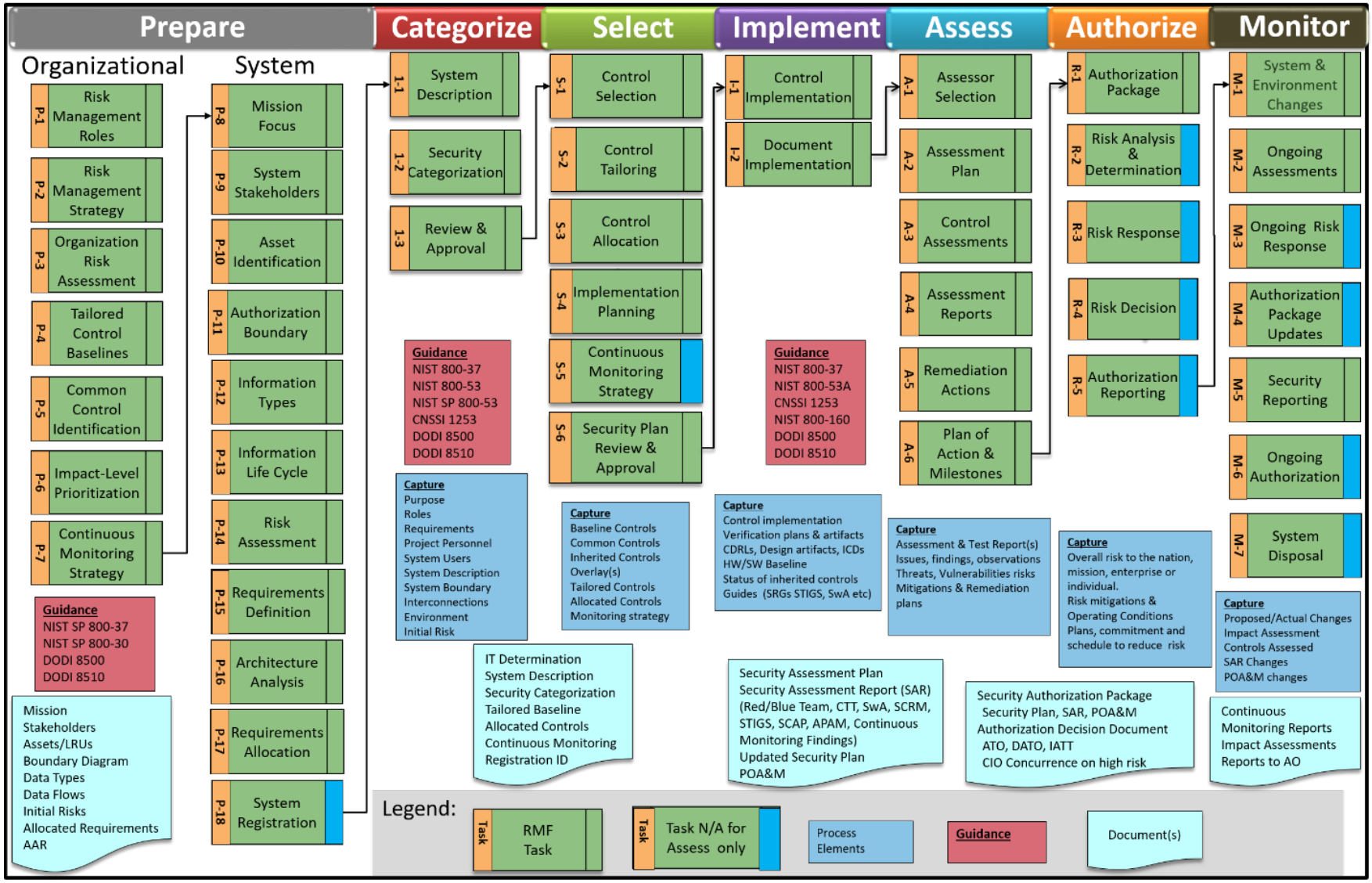


FIGURE G-1: RMF Process

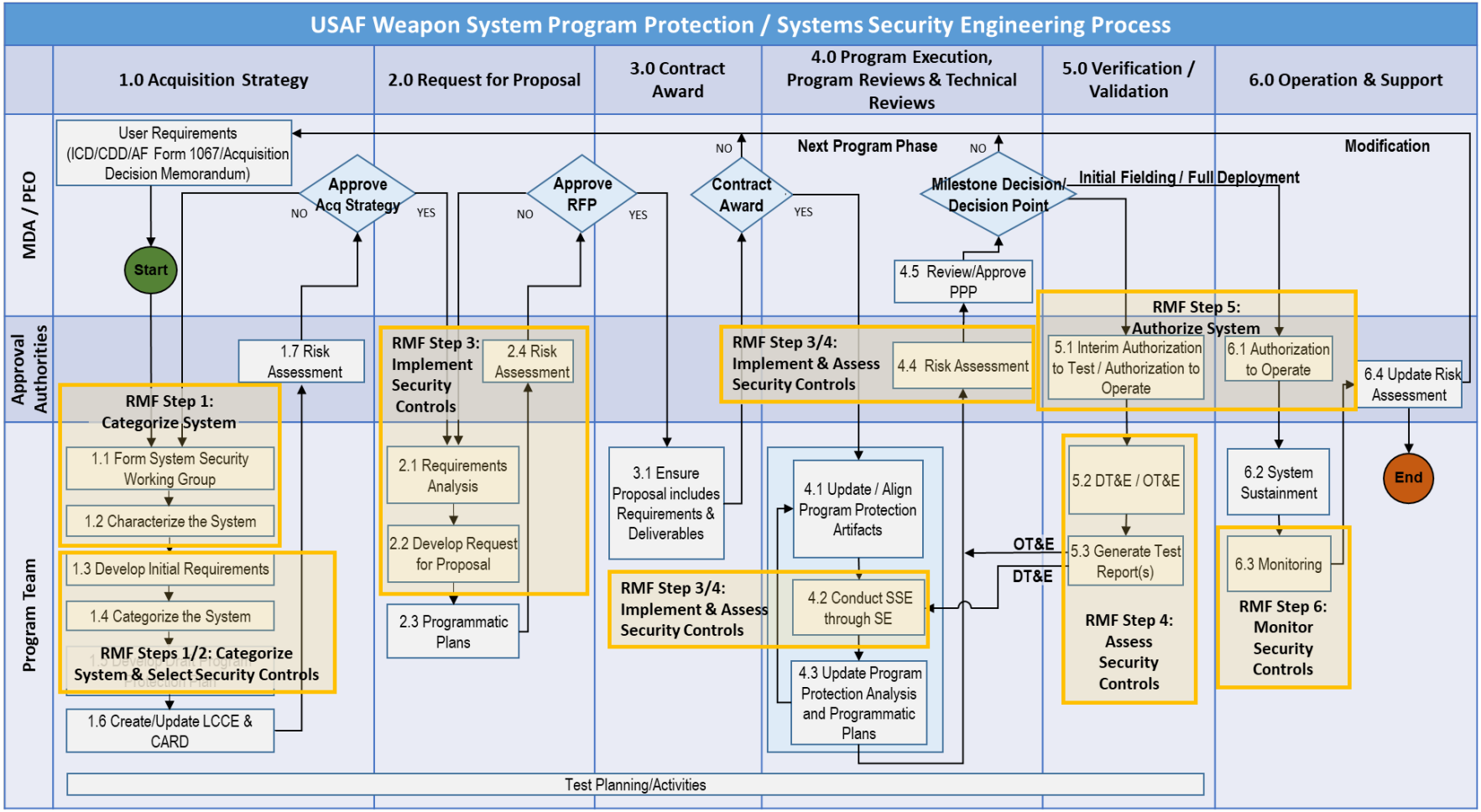


FIGURE G-2: USAF Weapon System PP/SSE Process.

A more detailed mapping of the RMF steps to the PP/SSE process steps in Table G-1 of this document is below.

Table G-1: Trace between RMF Steps and USAF Weapon System PP/SSE Guidebook WBS Steps.

RMF Step	PP/SSE WBS Step
RMF: Prepare	
P-1	
P-2	
P-3	1.7, 2.4
P-4	
P-5	
P-6	
P-7	
P-8	1.1.4, 1.2.3, 1.2.6, 1.2.7, 1.3.3.5, 1.5.1
P-9	
P-10	
P-11	1.1.5, 1.2.4
P-12	1.2.5, 1.4.1, 1.5.1
P-13	
P-14	1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.5.3, 1.7, 2.4
P-15	1.1.3, 1.2.1, 1.2.8, 1.3.6, 1.6
P-16	1.3.2.2, 1.5.4, 4.2.2, 4.2.12
P-17	1.3.6, 2.1.1, 2.1.2, 2.2.1, 2.2.2, 2.2.3
P-18	1.3.4
RMF: Categorize	
1-1	1.2.2
1-2	1.4.2
1-3	1.4.3
RMF: Select	
S-1	1.3, 4.2
S-2	1.3, 4.2
S-3	1.3, 4.2
S-4	2.0

S-5	2.3, 4.1.4, 4.5
RMF: Implement	
I-1	4.2
I-2	1.5.4, 4.2, 4.3
RMF: Assess	
A-1	1.1.1, 4.2
A-2	2.3, 4.1.4, 4.2.8, 5.2.1
A-3	5.2.2, 5.2.3
A-4	4.4, 5.3
A-5	5.1.2
A-6	4.3.1
RMF: Authorize	
R-1	5.1.1
R-2	5.1.2
R-3	5.1.2
R-4	5.1.2, 6.1
R-5	5.1, 6.1
RMF: Monitor	
M-1	6.3.9
M-2	6.3.1, 6.3.8
M-3	6.3.2
M-4	6.4
M-5	6.3.3
M-6	6.4
M-7	6.3.4

1.2 PP/SSE Process and Test and Evaluation (specifically the Mission Based Cyber Risk Assessment)

Figure G-3 shows the alignment between the PP/SSE Process and T&E activities. The boxes circled in red highlight Test & Evaluation involvement or activities. The boxes highlighted in yellow indicated where inputs to and updates to the Mission Based Cyber Risk Assessment (MBCRA) will be completed. More guidance on the MBCRA can be found in the DoD Cybersecurity Test and Evaluation Guidebook.

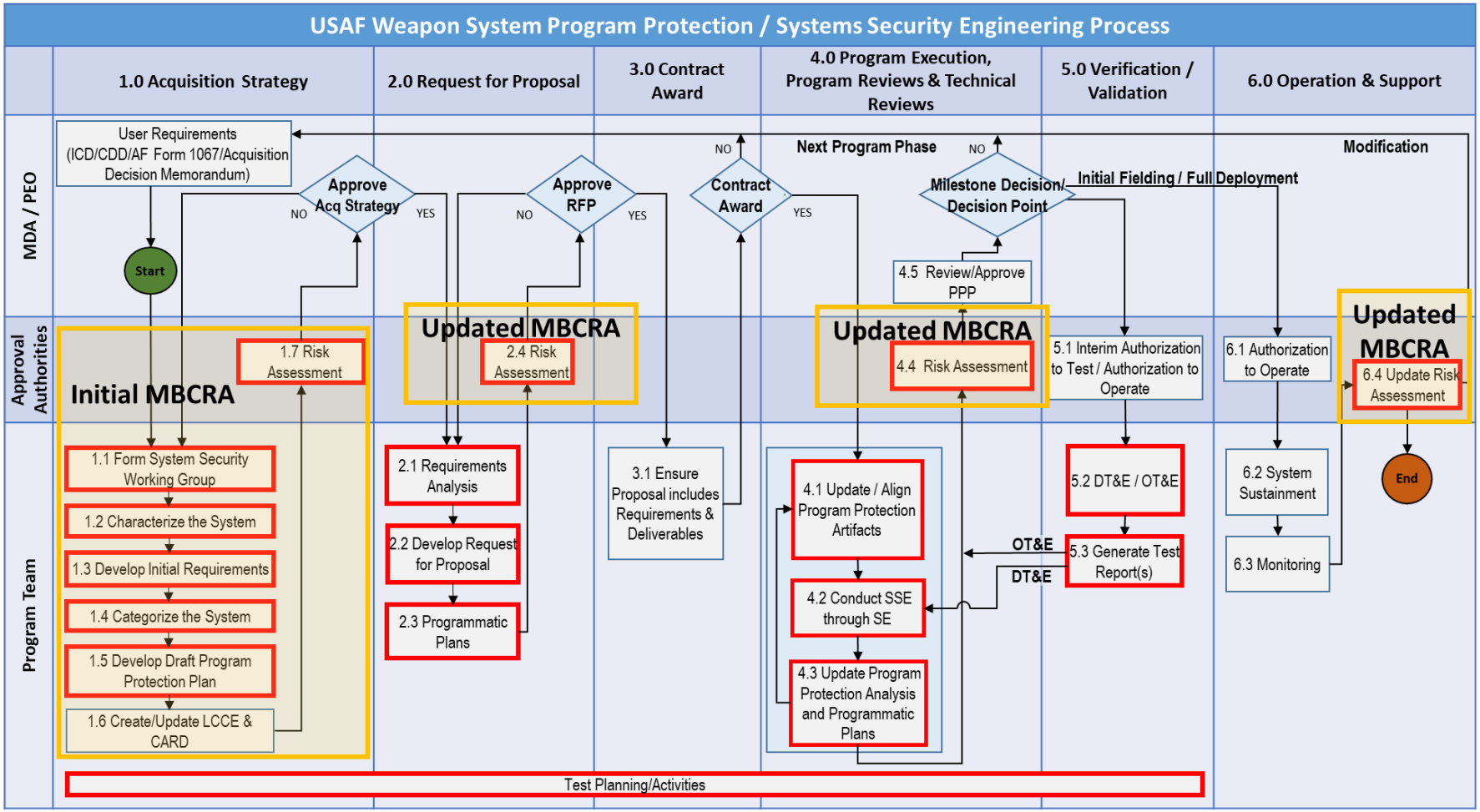


FIGURE G-3: USAF Weapon System PP/SSE Process and Test and Evaluation.

APPENDIX H – 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 (Ref. 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 (Ref. DoDI 5200.39).

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 exfiltrating 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 SP 800-39).

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 (Ref. DOT&E TEMP Guidebook).

Adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities (Ref. CNSSI No. 4009, NIST SP 800-39).

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 http://farsite.hill.af.mil/vmaffara.htm.

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 (Ref. DoDD 5200.47E).

Anti-Tamper Executive Agent (ATEA): The DoD ATEA is 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 (OUSD (AT&L)) (Ref. DoDI 5200.39, Headquarters AF Mission Directive 1-10).

Applicable Systems:

(1) 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;

(2) 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

(3) 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. (Ref. 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 (Ref. 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 (Ref. CNSSI No. 4009).

Capability: The ability to complete a task or execute a course of action under specified conditions and level of performance. (Ref. CJCSI 5123.01H).

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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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. (Ref. 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 (Ref. 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 (Ref. DoDI 5200.44).

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 (Ref. DoDI 5200.39).

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 (Ref. CNSSI No. 4009, NIST SP 800-60).

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) (Ref. 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. (Ref. CNSSI No. 4009).

Cyber (adj.): Of or pertaining to the cyberspace environment, capabilities, plans, or operations (Ref. AFPD 17-2).

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) (Ref. DoD PM's Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Lifecycle).

Cyber Incident: Actions taken through the use of 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 (Ref. 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 SP 800-160 vol 2). See also definition for "Resilience".

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (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 (Ref. JP 3-12R).

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 (Ref. DoDI 8500.01).

Cyber Survivability: The ability of a system to prevent, mitigate and recover from cyber-attacks. (Ref. paraphrased from the Manual for the Operation of the JCIDS). Within this Guidebook, 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 (Ref. 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 (Ref. 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 (Ref. JP 3-12R).

Embedded Information Technology: Computer resources, both hardware and software, which are an integral part of a weapon or weapon system (Ref. DoDI 5000.02).

Event: An observable occurrence in an information system or network (Ref. CNSSI No. 4009). Within this guidebook, "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 (Ref. 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 (Ref. NIST SP 800-171, Revision 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 (Ref. ISO/IEC/IEEE 29119-4:2015).

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 (Ref. DoDI 5200.39).

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).

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 (Ref. DoDI 5200.44).

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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. NIST SP 800-171).

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 (Ref. JP 3-0).

Measure of Performance (MOP): A criterion used to assess friendly actions that is tied to measuring task accomplishment (Ref. JP 3-0).

Mission: The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task (Ref. 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 (Ref. 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 (Ref. DoDI 5200.44). Mission Critical Functions are analogous to Mission Essential Functions.

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 (Ref. AFI 10-208). Mission Essential Functions are analogous to Mission Critical Functions.

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 (Ref. Software Engineering Institute).

Modification Sensitive: Protection from the adversary making modifications to the CPI within the system. (DoD Anti-Tamper Desk Reference)

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 (Ref. DoDI 8500.01).

Organic CPI: Unique CPI that is owned and generated by an RDT&E program (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. DoDI 8500.01).

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 (Ref. DoDI 5000.02, Enclosure 3, Item 13).

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.) (Ref. AFPAM 63-113).

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 (Ref. AFPAM 63-113).

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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. 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 (Ref. CNSSI No. 4009).

Security Control Assessor (SCA): The individual, group, or organization responsible for conducting a security control assessment (Ref. 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 (Ref. 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 (Ref. 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 (Ref. DoDI 8500.01).

Sight Sensitive: Protect the CPI from compromise or from the adversary seeing the CPI within the system (DoD Anti-Tamper Desk Reference).

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 (Ref. http://cwe.mitre.org).

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) (Ref. 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 (Ref. 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 (Ref. 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 (Ref. DoDI 4140.01 *DoD Supply Chain Materiel Management Policy*).

Survivability: All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy (Ref. JP 3-34).

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 (Ref. 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 (Ref. 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 (Ref. DoDI 5000.02).

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 (Ref. 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 (Ref. 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 (Ref. CNSSI No. 4009).

Threat Event: An event or situation that has the potential for causing undesirable consequences or impact (Ref. NIST SP 800-30).

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 (Ref. 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).

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 I – Acronym List

Acronym	Definition
A&AS	Advisory and Assistance Services
A/D	Analog to Digital
AA	Adversarial Assessment
ACAT	Acquisition Category
ACD	Adversarial Cybersecurity Developmental Test and Evaluation
ACE	Acquisition Center of Excellence
ACL	Access Control List
ACTA	Adversary Cyber Threat Analysis
ADM	Acquisition Decision Memorandum
AFFARS	Air Force Federal Acquisition Regulation 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
AIG	Acquisition Intelligence Guide
AO	Authorizing Official
AoA	Analysis of Alternatives
AP	Acquisition Plan
ARRT	Acquisition Requirements Roadmap Tool
AS	Acquisition Strategy
ASAC	Application of Software Assurance Countermeasures
ASDB	Acquisition Security Database
ASIC	Application-Specific Integrated Circuit
ASICS	Application Specific Integrated Circuits
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
BOE	Body of Evidence
BOM	Bill of Materials
C2	Command And Control

CA	Criticality Analysis
CAC	Common Access Card
CAPEC™	Common Attack Pattern Enumeration and 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
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDS	Cross Domain Solution
CE	Chief Engineer
CI	Configuration Item; Counterintelligence
CICC	Cyber Incident Coordination Cell
CIO	Chief Information Officer
CISP	Counterintelligence Support Plan
CLO	Counter Low Observable
CMMI®	Capability Maturity Model Integration®
CMMI-DEV	Capability Maturity Model Integrated for Development
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CoC	Certificate of Conformance
CofC	Consequence of Compromise
COI	Community of Interest
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial off the Shelf
CPI	Critical Program Information
CPM	Capability Portfolio Management
CRM	Comment Resolution Matrix
CROWS	Cyber Resiliency Office for Weapon Systems
CR-TAC	Cyber Resiliency Technical Advisory Council
CS	Cybersecurity Strategy
CSA	Cyber Survivability Attributes
CSAR	Cybersecurity 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
CSSLP	Certified Secure Software Lifecycle Professional
CSSP	Cybersecurity Service Provider
CT	Critical Technologies
CTA	Capstone Threat Assessment
CTE	Critical Technology Element
CTI	Controlled Technical Information

CUI	Controlled Unclassified Information
CV-	Capability Viewpoint
CVE®	Common Vulnerabilities and Exposures
CVI	Cooperative Vulnerability Identification
CVPA	Cooperative Vulnerability and Penetration Assessment
CWBS	Contractor Work Breakdown Structure
CWE™	Common Weakness Enumeration
CyWG	Cyber Working Group
D/A	Digital to Analog
DAB	Defense Acquisition Board
DAE	Defense Acquisition Executive
DAG	Defense Acquisition Guidebook
DASD(SE)	Office of the Deputy Assistant Secretary of Defense for Systems Engineering
DAU	Defense Acquisition University
DCO	Defensive Cyberspace Operations
DCSA	Defense Counterintelligence and Security Agency (DCSA)
DCS	Direct Commercial Sales, Distributed Control System
DEF	Defense Exportability Features
DFARS	Defense Federal Acquisition Regulations System
DIA	Defense Intelligence Agency
DIA-TAC	Defense Intelligence Agency Threat Assessment Center
DID	Data Item Description
DISA	Defense Information Systems Agency
DITPR	Department of Defense Information Technology Portfolio Registry
DMEA	Defense Microelectronics Agency
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DOT&E	Director Operational Test & Evaluation
DR	Deficiency Report
DSS	Defense Security Service
DSTL	Defense Science and Technology List
DT	Developmental Test
DT&E	Developmental Test and Evaluation
E3	Electromagnetic Environmental Effects
EAR	Export Administration Regulations
ECR	Export Control Reform
ECU	End Cryptographic Unit
EI	Engineering Instruction
EITDR	Enterprise Information Technology Data Repository
ELA	Enterprise Licensing Agreement
eMASS	Enterprise Mission Assurance Support Service

EMD	Engineering and Manufacturing Development
EMS	Enterprise Master Schedule
EO/IR	Electro-Optical/Infrared
ESI	Enterprise Software Initiative
ESLOC	Equivalent Source Lines Of Code
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 and Development Center
FGPA	Field Programmable Gate Array
FIPS	Federal Information Processing Standards
FMEA	Failure Modes and Effects Analysis
FMS	Foreign Military Sales
FOSS	Free and Open Source Software
FOUO	For Official Use Only
FPGA	Field-Programmable Gate Array
FQT	Factory Qualification Test
FRP	Full Rate Production
FRP/FD	Full-Rate Production/Full-Deployment
FSM	Firmware Support Manual
FTA	Fault Tree Analysis
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
HPT	High Performance Team
HW	Hardware
HwA	Hardware Assurance
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
ICD	Initial Capabilities Document; Interface Control Document
ICT	Information and Communications Technology
IdAM	Identity and Access Management
IDD	Interface Design Document
IDS	Intrusion Detection System
IE	Information Enterprise

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILC	Integrated Life Cycle
IMS	Integrated Master Schedule
INCOSE	International Council on Systems Engineering
INFOSEC	Information Security
IO	Information Operations
IOT&E	Initial Operational Test and Evaluation
IP	Information Protection; Internet Protocol; Intellectual Property
IPMR	Integrated Program Management Report
IPT	Integrated Product Team
IPv6	Internet Protocol Version 6
IR&D	Independent Research and Development
IRT	Incident Response Team
ISO	Information Security Officer
ISP	Information Support Plan
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
IT	Information Technology
ITA	Integrated Threat Assessment
ITAR	International Traffic in Arms Regulation
ITCC	Information Technology Commodity Council
ITIPS	Information Technology Investment Portfolio System
IUID	Item Unique Identification
JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration Development System
JCS	Joint Chiefs of Staff
JDRS	Joint Deficiency Requirements System
JELA	Joint Enterprise Licensing Agreement
JFAC	Joint Federated Assurance Center
JIE	Joint Information Environment
JITC	Joint Interoperability and Test Command
JP	Joint Publication
KCMP	Key and Certificate Management Infrastructure
KMI	Key Management Infrastructure
KMP	Key Management Plan
KPP	Key Performance Parameter
KS	Knowledge Service
KSA	Key System Attribute
LBC	Logic Bearing Components
LCSP	Lifecycle Sustainment Plan
LDTO	Lead Developmental Test Organization
LE	Lead Engineer
LO	Low Observable
LOA	Line of Action; Letter of Agreement
LRU	Line Replaceable Unit

MCF	Mission critical Function
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MOAs	Memoranda of Agreement
MOE	Measures Of Effectiveness
MOP	Measures Of Performance
MOUs	Memoranda of Understanding
MS	Milestone
NAR	Non-Advocate Review
NASIC	National Air and Space Intelligence Center
NCES	Net-Centric Enterprise Services
NdA	Non-Disclosure Agreement
NDAA	National Defense Authorization Act
NDI	Non-Developmental Item
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 and Technology
NRE	Non-Recurring Engineering
NSA	National Security Agency
NSS	National Security Systems
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
O&M	Operations and Maintenance
O&S	Operations and Support
OCM	Original Component Manufacturer
OEM	Original Equipment Manufacturer
OFP	Operational Flight Program
OMG	Object Management Group
OMS	Open Mission Systems
OPSEC	Operations Security
OS	Operating System
OSD	Office of the Secretary of Defense
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTO	Operational Test Organization
OTRR	Operational Test Readiness Review
OTS	Off-The-Shelf
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
OV-	Operational Viewpoint
OWASP	Open Web Application Security Project
P&D	Production and Deployment

PBA	Performance-Based Agreement
PCA	Physical Configuration Audit
PD	Production and Deployment
PDR	Preliminary Design Review
PEO	Program Executive Officer
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
PMR	Program Management Review
PNT	Positioning, Navigation and Timing
PO	Program Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POM	Program Objectives Memorandum
PP	Program Protection
PPBE	Planning, Programming, Budgeting and Execution
PPIP	Program Protection Implementation Plan
PPP	Program Protection Plan
PPS	Program Protection Survey
PR	Production Requirement
PROM	Programmable Read-Only Memory
PSS	Product Support Strategy
PWS	Performance Work Statement
QEB	Quantum Enterprise Buy
R&D	Research and Development
RAM	Random Access Memory; Reliability, Availability and Maintainability
R-CPI	Resident-Critical Program Information
RDT&E	Research, Development, Test, and Evaluation
RE	Reverse Engineering
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposal
RMB	Risk Management Board
RMF	Risk Management Framework
RMP	Risk Management Plan
ROM	Read-Only Memory; Rough Order of Magnitude
RVM	Requirements Verification Matrix
RWG	Risk Working Group
SA	Situational Awareness
SACM	Structured Assurance Case Metamodel
SAE	Service Acquisition Executive
SAF-AQL	Secretary of the Air Force, Acquisition and Logistics
SAPF	Special Access Program Facility

SAP	Security Assessment Plan; Special Access Program
SAR	Security Assessment Report
SAT	Site Acceptance Test
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SCAP	Secure Content Automation Protocol
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 and Life Cycle Support
SEI	Software Engineering Institute
SEI&T	Systems Engineering, Integration, and Test
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Plan
SETA	Systems Engineering and Technical Assistance
SETR	Systems Engineering Technical Review
SF	Standard Form
SFR	System Functional Review
SFY	Safe Array
SHP	Security Handling Plan
SIPRNet	Secret Internet Protocol Router Network
SLOC	Source Lines Of Code
SME	Subject Matter Expert
SOO	Statement of Objectives
SoS	Sources of Suppliers
SOW	Statement of Work
SP	Security Plan; Standard Process; Special Publication
SRD	System Requirements Document
SRG	Security Requirements Guide
SRR	System Requirements Review
SRS	Software Requirements Specification
SRU	System Replaceable Unit
SS	System Specification
SSC	Single Chip Crypto
SSDD	System/Segment Design Document
SSE	Systems Security Engineering
SSEB	Source Selection Evaluation Board
SSS	Staff Summary Sheet
SSWG	Systems Security Working Group
STAR	System Threat Assessment Report

STIG	Security Technical Implementation Guide
STP	Software Test Plan
STR	Software Test Report
SV-	Systems Viewpoint
SVR	System Verification Review
SVT	Security Verification Test
SW	Software
SwA	Software Assurance
SWAMP	Software Acquisition Management Plan
T&E	Test and Evaluation
TA/CP	Technology Assessment/Control Plan
TAC	Threat Assessment Center
TD	Technology Development
TDY	Temporary Duty
TDS	Technology Development Strategy
TEMP	Test and Evaluation Master Plan
TEMP	Test and Evaluation Master Plan
TIG	Technical Implementation Guidebook
TMRR	Technology Maturation and Risk Reduction
TO	Technical Order; Task Order
TPI	Technical Performance Indicators
TPM	Technical Performance Measure
TRA	Technology Readiness Assessment
TRANSEC	Transmission Security
TRL	Technology Readiness Level
TRR	Test Readiness Review
TS	Top Secret
TSN	Trusted Systems and Networks
TSRD	Telecommunications Security Requirements Document
U.S.C.	United States Code
UCI	Universal Command and Control Interface
URL	Uniform Resource Locator
US	United States
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Response Team
USCYBERCOM	United States Cyber Command
USD(AT&L)	Undersecretary of Defense for Acquisition, Technology and Logistics
USD(P)	Under Secretary of Defense for Policy
USML	United States Munitions List
VHDL	Very-High-Speed-Integrated-Circuits (VHSIC) Hardware Description Language
VOIP	Voice-over-Internet-Protocol
VOLT	Validated On-Line Life Cycle Threat
WARM	Wartime Reserve Mode
WBS	Work Breakdown Structure

APPENDIX J – References

Law

- National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2011, Section 806
- National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012, Section 818
- National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, Section 833
- National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2014, Section 803
- National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2015, Section 231
- National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23, “Cybersecurity Policy,” 08 Jan 2008
- Public Law 111-383 (FY11 NDAA, Section 932): Strategy on Computer Software Assurance
- U.S. Code Title 41, Public Contracts, Chapter 7, Office of Federal Procurement Policy
- U.S. Code Title 40, Clinger-Cohen Act
- U.S. Code, Title 44, Para 3541, Federal Information Security Management Act

Policy

- AFI 10-601, “Operational Capability Requirements Development”, 6 Nov 2013
- AFI 16-1404, “Air Force Information Security Program,” 29 May 2015
- AFI 16-1406, “Air Force Industrial Security Program,” 25 Aug 2015, Incorporating Change 1, 30 Jan 2017
- AFI 17-101, “Risk Management Framework (RMF) for Air Force (AF) Information Technology,” 02 Feb 2017
- AFI 17-130, “Cyberspace Program Management,” 16 Feb 2016
- AFI 17-140, “Architecting”, 29 Jun 2018
- AFI 17-202_AFGM2016-01, “Cyber Incident Handling,” 05 Jul 2016
- AFI 63-101/20-101, “Integrated Lifecycle Management,” 09 May 2017
- AFI 64-102, "Operational Contracting Program,” 09 Oct 2014
- AFI 90-802, “Risk Management,” 1 Apr 2019
- AFLCMC Standard Process for Cybersecurity Assessment and Authorization v3.1, 17 Oct 2019 https://cs2.eis.af.mil/sites/21710/gov/APDSP/Forms/AllItems.aspx
- AFMAN 14-401, “Intelligence Analysis And Targeting Tradecraft/Data Standards,” 8 Aug 2019
- AFMAN 17-1203, "IT Asset Management (ITAM),” 1 Apr 2019
- AFMAN 17-1301, “Computer Security (COMPUSEC),” 10 Feb 2017
- AFMAN 17-1303, “Cybersecurity Workforce Improvement Program,” 9 Aug 2019
- AFMAN 17-1402, “Air Force Clinger Cohen Act Compliance Guide,” 20 Jun 2018
- AFPAM 63-113, "Program Protection Planning for Lifecycle Management,” 17 Oct 2013
- AFPAM 63-128, “Integrated Lifecycle Management,” 10 Jul 2014
- AFPAM 90-803, “Risk Management Guidelines and Tools,” 3 Mar 2017
- AFPD 17-2, “Cyberspace Operations,” 12 Apr 2016
- AFPD 63-1, “Integrated Lifecycle Management,” 03 Jun 2016, 6 Aug 2018
- AFPD 64-1, "The Contracting System,” 5 Nov 2018
- CJCSI 5123.01H “Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS),” 31 Aug 2018

- CJCSM 6510.01b, “Cyber Incident Handling Program” 18 Dec 2014
- CJCSI 6510.01f, “Information Assurance (IA) and Support to Computer Network Defense (CND)” 9 June 2015
- CNSSD No. 505, “Supply Chain Risk Management (SCRM),” 07 Mar 2012
- CNSSP No. 11, “Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,” 01 Jun 2013
- CNSSP No. 22, “Information Assurance Risk Management Policy for National Security Systems,” 01 Jan 2012
- CNSSP No. 28, “Cybersecurity of Unmanned National Systems”, 6 Jul 2018
- CNSSI No. 1253, “Security Categorization and Control Selection for National Security Systems,” 27 Mar 2014
- CNSSI No. 1253F, “Overlays,” Attachments 1-6
- CNSSI No. 1254, “Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems,” 31 Aug 2016
- DoD O-5205.13, “Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program Security Classification Manual (SCM),” 26 Apr 2012, Incorporating Change 2, 21 Aug 2019
- DoD 5220.22-M, “National Industrial Security Program Operating Manual,” 28 Feb 2006, Incorporating Change 2, 18 May 2016
- DoD 8570.01-M, "Information Assurance Workforce Improvement Program,” 19 Dec Incorporating Change 4, 10 Nov 2015
- DoDD 3020.40, “Mission Assurance,” 29 Nov 2016, Incorporating Change 1, 11 Sep 2018
- DoDD 5200.47E, “Anti-Tamper (AT),” 4 Sep 2015, Incorporating Change 2, 31 Aug 2015
- DoDD 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations,” 16 Jun 1992
- DoDI 4140.01, “DoD Supply Chain Materiel Management Policy,” 6 Mar 2019
- DoDI 4140.67, “DoD Counterfeit Prevention Policy,” 26 Apr 2013, Incorporating Change 2, 31 Aug 2018
- DoDI 5000.02, “Operation of the Defense Acquisition System,” 07 Jan 2015, Incorporating Change 5, 21 Oct 2019
- DoDI 5000.02, ENCL 14, “Cybersecurity in the Defense Acquisition System,” 7 Jan 2015, Incorporating Change 5, 21 Oct 2019
- DoDI 5000.35, "Defense Acquisition Regulations (DAR) System,” 21 Oct 2008, Incorporating Change 2, 31 Aug 2018
- DoDI 5000.73, “Cost Analysis Guidance and Procedures,” 09 Jun 2015, Incorporating Change 1, 2 Oct 2017
- DoDI 5200.39, “Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E),” 28 May 2015, Incorporating Change 2, 15 Oct 2018
- DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),” 05 Nov 2012, Incorporating Change 2, 15 Oct 2018
- DoDI S-5230.28, “Low Observable (LO) and Counter Low Observable (CLO) Programs,” 26 May 2005, Incorporating Change 1, 21 Aug 2018
- DoDI 8320.04, “Item Unique Identification (IUID) Standards for Tangible Personal Property,” 03 Sep 2015, Incorporating Change 3, 27 Aug 2017
- DoDI 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” 21 May 2014, Incorporating Change 1, 18 Dec 2017
- DoDI 8500.01, “Cybersecurity,” 14 Mar 2014, Incorporating Change 2, 28 Jul 2017

- DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” 12 Mar 2014, Incorporating Change 2, 28 Jul 2017
- DoDI 8530.01, “Cybersecurity Activities Support to DoD Information Network Operations,” 07 Mar 2016, Incorporating Change 1, 27 Jul 2017
- DoDI 8540.01, “Cross Domain Policy,” 8 May 2015, Incorporating Change 1, 28 Jul 2017
- DoDI 8581.01, “IA Policy for Space Systems Used by the Department of Defense,” 08 Jun 2010
- DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," 6 Jun 2012, Incorporating Change 1, 27 Oct 2017
- DoDM S-5230.28, “Policy for Low Observable (LO) and Counter Low Observable (CLO) Programs", 28 Dec 2016
- DoDM 5220.22, Volume 2, “National Industrial Security Program: Industrial Security Procedures for Government Activities”, 1 Aug 2018
- DoDM 4140.01, Volume 1,”DoD Supply Chain Materiel Management Procedures: Operational Requirements,” 10 Feb 2014
- FIPS 140-2, “Security Requirements for Cryptographic Modules,” with change notices 03 Dec 2002
- FIPS 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” Aug 2013
- Headquarters AF Mission Directive 1-10, 8 Apr 2010
- JP 3-0, “Joint Operations,” 17 Jan 2017
- JP 3-12 (R), “Cyberspace Operations,” 05 Feb 2013
- JP 3-34, “Joint Engineer Operations,” 06 Jan 2016
- NIST SP 800-30, “Guide for Conducting Risk Assessments,” Rev 1, Sep 2012
- NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems,” Dec 2018 (as amended)
- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View,” Mar 2011
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 4, Dec 2014, Incorporating Changes 22 Jan 2015
- NIST SP 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” Sep 2011
- NIST SP 800-160, “Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems,” Nov 2016 (as amended)
- NIST SP 800-160 Volume 2, “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”, Nov 2019
- NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” Apr 2015
- NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” Rev. 1, 7 June 2018
- NSTISSAM TEMPEST/1-92, “Compromising Emanations Laboratory Test, Electromagnetics,” 15 Dec 1992
- White House Office of Management and Budget Circular No. A-130, “Managing Information as a Strategic Resource”, 27 July 2016, https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

Guidance

- Aerospace TOR-2006(1455)-5743 REV B, “Software Acquisition Management Plan Preparation Guide,” 27 Sep 2011
- Aerospace TOR-2013-00825, “Program Protection Plan Content Rich Template,” 30 Sep 2013
- Aerospace TOR-2014-02828, “Integrating Software Assurance into the Request for Proposal (RFP),” 22 Sep 2014
- Aerospace TOR-2015-00012, “Software Development Standard for Mission Critical Systems,” 17 Mar 2015
- AF CIO “AF Program Manager’s Guide for Developing and Processing Information Support Plans and Associated Interoperability Guidance,” 26 Jan 2016
- AF Life Cycle Management Center Engineering Model Request for Proposal (AFLCMC EM-RFP)
- AF Life Cycle Management Center Standard Process for Cybersecurity Assessment and Authorization
- Anti-Tamper Security Classification Guide - https://at.dod.mil/
- Carnegie Mellon University Software Engineering Institute CMU/SEI-2009-TR-010, “Secure Design Patterns,” Oct 2009 http://www.sei.cmu.edu/reports/09tr010.pdf
- Carnegie Mellon University Software Engineering Institute CMU/SEI-2018-SR-025, “Program Manager’s Guidebook for Software Assurance”, Dec 2018 https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_538779.pdf
- Carnegie Mellon University Software Engineering Institute CMU/SEI-2018-SR-013, “DoD Developer’s Guidebook for Software Assurance, Dec 2018 https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_538761.pdf
- Common Attack Pattern Enumeration and Classification (CAPEC™) https://capec.mitre.org/
- Common Vulnerabilities and Exposures (CVE®) https://cve.mitre.org/
- Common Weakness Enumeration (CWE™) http://cwe.mitre.org/
- “CPI Assessment and Identification Guide (CAIG) v. 1.0,” NDIA, 2 Aug 2019 (FOUO) https://at.dod.mil/
- “CPI/LO/CLO Workbook Template 1.0”, NDIA, 2 Aug 2019 (FOUO) https://at.dod.mil/
- “CPI/LO/CLO Workbook Template 1.0 - Classified HPG and 5230 Tabs,” 2 Aug 2019 (SECRET), document request through https://at.dod.mil/
- CWE/SANS TOP 25 Most Dangerous Programming Errors https://www.sans.org/top25-software-errors/
- Cybersecurity SCDG for Air Force Weapon Systems https://www.dtic.mil/DTICOnline/home.search
- Defense Acquisition Guidebook (DAG), Chapter 6-3.10.1, “Cybersecurity”
- Defense Acquisition Guidebook (DAG), Chapter 9, “Program Protection”
- Defense Acquisition Guidebook (DAG), Chapter 9-3.2.1, “Anti-Tamper”
- Defense Acquisition Guidebook (DAG), Chapter 3-4.3.24, “System Security Engineering”
- Defense Acquisition Guidebook (DAG), Chapter CH 9–3.3 “Engineering Design Activities”
- Defense Acquisition Guidebook (DAG), Chapter CH 9–4.1 “Contracting for Program Protection”
- Defense Acquisition Guidebook (DAG), Chapter 10, "Acquisition of Services"
- Defense Counterintelligence and Security Agency, “DSS Assessment and Authorization Process Manual (DAAPM),” Version 1.1, 31 March 2017
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), “Program Protection Plan Outline & Guidance,” Jul 2011

- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), “Program Protection Plan Evaluation Criteria,” Feb 2014
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) and Department of Defense Chief Information Officer (DoD CIO), “Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals,” Jan 2014
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), "Guidance to Requiring Activities for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information),” Feb 2015
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), “Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs,” Jan 2017
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), “DoD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle,” Version 1.0, 30 Oct 2015
- Deputy Assistant Secretary of Defense for Systems Engineering (SASD(SE)) and DoD Chief Information Officer (CIO) “Software Assurance Countermeasures in Program Protection Planning,” March 2014 https://ac.cto.mil/wp-content/uploads/2019/06/SwA-CM-in-PPP.pdf
- DoD Anti-Tamper Security Classification Guide (SCG) and Safe Array (SFY) Compartment Security Classification Guide, 30 Sep 2015
- DoD Anti-Tamper Desk Reference, Second Edition, April 2017(FOUO document)
- DoD Anti-Tamper (AT) Guidelines, 30 Nov 2016 (SECRET document)
- DoD Cyber Discipline Implementation Plan, Feb 2016
- DoD Cybersecurity Test and Evaluation (T&E) Guidebook, Version 1.0, 01 Jul 2015
- DOD Operational Test and Evaluation (DOT&E) TEMP Guidebook, Version 3.1, 19 Jan 2017
- DoD Software Assurance (SwA) Community of Practice (CoP) Contract Language Working Group, “Suggested Language to Incorporate Software Assurance into DoD Contracts,” Feb 2016
- Director Operational Test and Evaluation (DOT&E) Memo, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs,” 3 April 2018 https://www.dote.osd.mil/pub/policies/2018/20180403ProcsForOTEofCybersecurityInAcqProgs(17092).pdf
- INCOSE Systems Engineering Handbook, Fourth Edition, Chapter 10.11, “Systems Security Engineering,” 2015
- IEEE Standard 1517-2010, “System and Software Life Cycle Processes--Reuse Processes,” 25 Aug 2010
- ISO/IEC 12207-2008, “Systems and Software Engineering -- Software Life Cycle Processes,” Jan 2008
- ISO/IEC 15026-1:2013, “Systems and Software Engineering -- Systems and Software Assurance -- Part 1: Concepts and Vocabulary”, Nov 2013
- ISO/IEC 15408-1:2009, “Security Techniques -- Evaluation Criteria for IT Security -- Part 1: Introduction and General Model,” 06 Jan 2014
- ISO/IEC 17050-1:2004, “Conformity Assessment -- Supplier's Declaration of Conformity -- Part 1: General Requirements,” Jun 2007
- ISO/IEC 17050-2:2004, “Conformity Assessment -- Supplier's Declaration of Conformity -- Part 2: Supporting Documentation,” Oct 2004

- ISO/IEC 21827:2008, "Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)," Oct 2008
- ISO/IEC/IEEE Standard 15288, "Systems and Software Engineering," 05 May 2015
- ISO/IEC/IEEE Standard 15288.1, "IEEE Standard for Application of Systems Engineering on Defense Programs"
- ISO/IEC/IEEE Standard 15288.2, "IEEE Standard for Technical Reviews and Audits on Defense Programs"
- ISO/IEC/IEEE 29119-4:2015, "Software and Systems Engineering – Software Testing (Part 4)," Dec 2015
- Joint Chiefs of Staff, "Cyber Survivability Endorsement Implementation Guide (CSEIG)," version 1.01 (FOUO)
- MIL-HDBK-1785, "System Security Engineering Program Management Requirements," 01 Aug 1995
- MIL-STD-881D, "Work Breakdown Structures for Defense Materiel Items," 09 Apr 2018
- MIL-STD-882E, "System Safety," 11 May 2012
- MIL-STD-961E, "Defense And Program-Unique Specifications Format And Content," Change 3, 27 Oct 2015
- MIL-STD-3018(2), "Parts Management," 02 Jun 2015
- NIST Security Content Automation Protocol (SCAP) https://scap.nist.gov/
- Office of the Under Secretary of Defense for Acquisition and Sustainment (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, link to memo: https://www.acq.osd.mil/dpap/pdi/cyber/docs/Guidance_for_Assessing_Compliance_and_Enhancing_Protections.pdf, link to attachment: https://www.acq.osd.mil/dpap/pdi/cyber/docs/Assess%20Compliance%20and%20Enhance%20Protection%20of%20Contractor%20System%20%20with%20Attachments%2011-6-2018.pdf
- OUSD(AT&L), "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle," May 2015
- OUSD(AT&L) Memorandum, "Defense Exportability Features Policy Implementation Memorandum and Guidelines," 09 April 2015
- OWASP Top 10 Most Critical Web Application Security Risks (OWASP Top 10) https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- SAE AS5553B, "Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition," 12 Sep 2016
- SAE AS9120B, "Quality Management Systems – Requirements for Aviation, Space, and Defense Distributors," 01 Nov 2016
- Sandia National Labs, "Tutorial on Anti-Tamper (AT) Protection Using Anti-Tamper (AT) Analysis/Synthesis," Version 1, 18 Apr 2005 (SECRET/NOFORN document)
- SCRM Program Management Office (PMO), "DoD Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management," 25 Feb 2010
- Secretary of the Air Force for Acquisition (SAF/AQ), "USAF Weapon Systems Software Management Guidebook," 15 Aug 2008
- Space and Missile Systems Center (SMC) Recommended Acquisition Language Guides
- The Open Web Application Security Project (OWASP) https://www.owasp.org

APPENDIX K – Comments Resolution Matrix (CRM)

Comments, suggestions, or questions on this document should be captured in the Comments Resolution Matrix (CRM) embedded below, and also located at: https://www.milsuite.mil/wiki/USAF_Acquisition_System_Security_Primer.

Blank CRM Template.docx

Email CRMs to the Cyber Resiliency Office for Weapon Systems (CROWS@us.af.mil).