

Air Force Life Cycle Management Center (AFLCMC)



Standard Process for Weapon System Program Protection Planning (PPP) & Systems Security Engineering (SSE)

16 July 2020

VERSION 3.0

Process Owner: AFLCMC/IP (Information Protection)

Distribution Statement D: Distribution authorized to DoD and U.S. DoD contractors only: Administrative or Operational Use, determined 29 Mar 2018. Other requests for this document shall be referred to AFLCMC/IP (AFLCMCIP.workflow@us.af.mil).

FOREWORD

- This AFLCMC Standard Process for Weapon System PPP & SSE is approved for use by all Program Executive Officers (PEOs) and programs under AFLCMC.
- To effectively execute the activities of this standard process 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:
<http://icatalog.dau.mil/onlinecatalog/CareerLvl.aspx#>
- Comments, suggestions or questions on this document should be captured on a Comments Resolution Matrix (CRM) form and emailed to the AFLCMC/IP Program Protection Team (AFLCMC.IPPPP.Workflow@us.af.mil). The CRM form is available at https://www.milsuite.mil/wiki/USAF_Acquisition_System_Security_Primer.
- Most of the content in the previous version of this Standard Process has been incorporated in the USAF Weapon System Program Protection / System Security Engineering Guidebook, which is available at:
<https://usaf.dps.mil/:w:/r/sites/CROWS/Shared%20Documents/CROWS%20Products/USAF%20Weapon%20System%20PP%20and%20SSE%20Guidebook%20v2.0.docx?d=weea95dad58484c9dace9991ac7e3875e&csf=1&web=1&e=t3wZwd>. Comments related to that guidebook should be directed to the Cyber Resiliency Office for Weapon Systems (CROWS) at CROWS@us.af.mil.

Record of Changes		
Version	Effective Date	Summary
1.0	16 Nov 2017	Basic Document; Approved by Standard Process Board on 16 Nov 2017
1.0	1 Dec 2018	Adopted by Air Force
1.0	1 Feb 2019	Integrated changes by Air Force and updated processes within AFLCMC
2.0	19 April 2019	Updates links; incorporates expanded PPP & SSE Coordination process; clarifies roles and responsibilities; and makes administrative changes. Approved by S&P Board on 19 April 2019.
3.0	16 July 2020	Annual Review; Removed all duplicated commentary that is now located and found in the USAF Weapon System PP/SSE Guidebook 2.0, 12 March 2020. Simplified the PPP coordination process in accordance with (IAW) the aforementioned USAF guidebook and integrated AFLCMC/IP additional requirements. Updated links and references. Cleaned up the acronym listing. Referenced emerging acquisition processes in addition to traditional schedules. Approved by the S&P Board, 16 July 2020.

Contents

1.0	Description	5
2.0	Scope	6
3.0	Entry and Exit Criteria for Program Protection Planning	8
4.0	Program Protection Plan Coordination and Approval	10
5.0	Roles and Responsibilities.....	12
6.0	Tools and Training.....	12
7.0	Definitions and Acronyms.....	13
8.0	References to Law, Policy, Instructions or Guidance.....	13
APPENDIX 1 – Attachments		16
APPENDIX 2 – Acronym Listing		17

1.0 Description

- 1.1 Program protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; hardware, software, and cyber vulnerability or supply chain exploitation; and battlefield loss throughout the system life cycle. The PPP process is required and executed iteratively across the acquisition life cycle in order to refine protection measures as the system matures. All new and legacy system programs, regardless of whether they have critical program information (CPI), must address mission critical components (CC) and functions as well as cybersecurity and cyber resilience, requiring risk management to protect critical technology information and capabilities. IAW AFI 63-101/20-101, *Integrated Life Cycle Management*, Chapter 6, program protection is a multi-functional activity to plan for and integrate holistic security policies and practices for AF programs throughout their life cycles. Note: Use of the term programs in Chapter 6 and in this Standard Process is not meant to limit application to acquisition category programs, it may be applied to systems, sub-systems, projects, or other acquisition activities. IAW 63-113, *Program Protection Planning for Life Cycle Management*, paragraph 1.4, all programs are required to perform protection planning; to include: ACAT programs, Technology Projects, and Special Access Programs. As noted in paragraph 1.4.1, PPP requirements for modifications can be satisfied by updating or annexing an existing PPP, creating a PPP for individual modification efforts, or creating a PPP for the entire weapon system with provisions for annexes to cover future modifications.
- 1.2 The goal is to address program protection early and throughout the system's life cycle to design in security and resiliency as the system design matures. As such, program protection informs and is informed by other aspects of defense acquisition; including contracting, test and evaluation, supply chain management, life cycle sustainment and depot management, intelligence, and system engineering constraints and decisions. The program protection process details how program offices will consciously address what needs to be protected and applies risk management processes to what cannot be adequately protected. The PPP should be a current and useable reference for understanding and managing the full spectrum of programs and systems security activities and system design tradeoffs. Finally, the PPP is updated as the system is developed, program critical assets are identified, and as threats or vulnerabilities change (or are better understood). It remains a living document required at Milestones A, B, C, the Development Request for Proposal (RFP) decision point, and the Full-Rate Production decision review, as described in DoDI 5000.02T, *Operation of the Defense Acquisition System* and DODI 5000.02, *Operation of the Adaptive Acquisition Framework*. It is a best practice to report progress to the Program Manager (PM) at each System Engineering Technical Review.
- 1.3 Figure 1 depicts the complexities of existing policy requirements program offices must currently navigate to accomplish program protection and System Security Engineering.

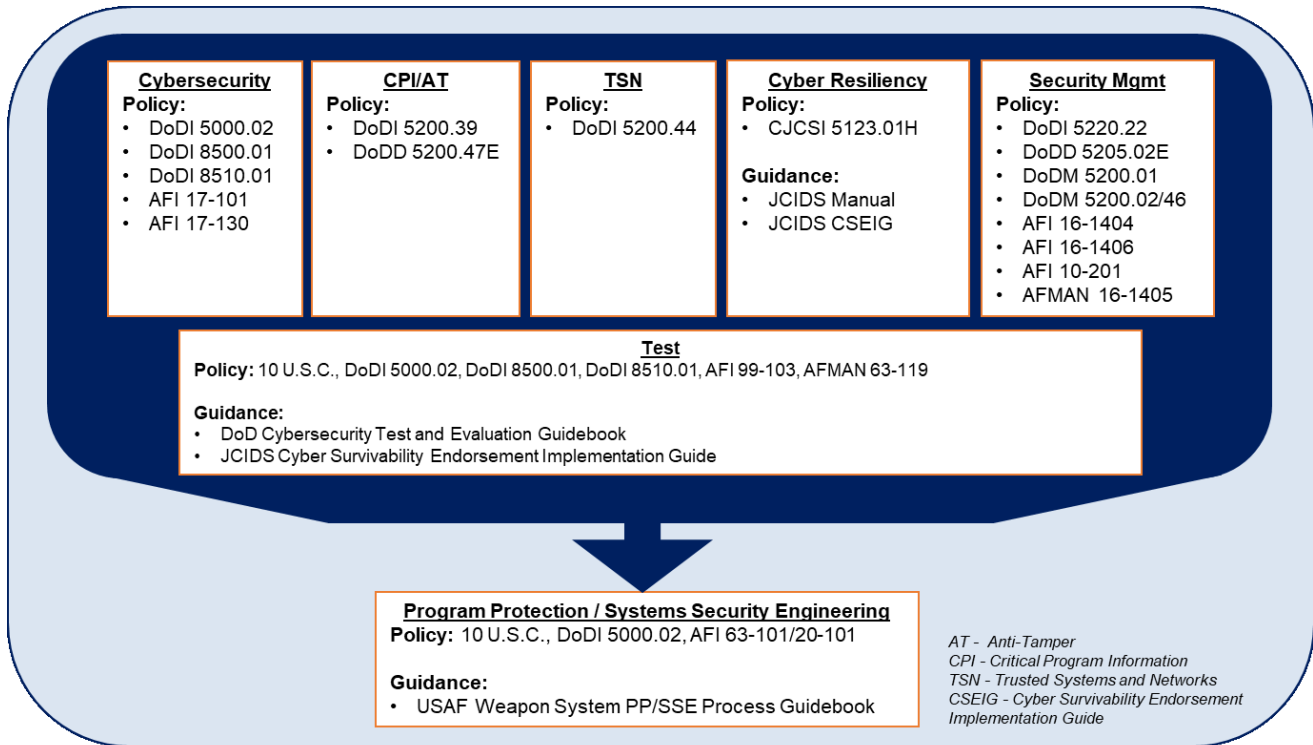


Figure 1: Program Protection and Systems Security Engineering Policy

2.0 Scope

- 2.1 The AFLCMC Standard Process for Weapon System PPP & SSE aligns with the USAF Weapon System PP and SSE Guidebook.
 - 2.1.1 Process Flowchart. The process flowchart previously found in this Standard Process has been incorporated into the USAF Weapon System Program Protection / System Security Engineering Guidebook.
 - 2.1.2 Work Breakdown Structure (WBS). The WBS previously embedded in this Standard Process has been incorporated into the USAF Weapon System Program Protection / System Security Engineering Guidebook.
 - 2.1.3 For an updated version of the USAF Weapon System PP/SSE Guidebook v2.0, refer to: <https://usaf.dps.mil/sites/21259/aflcmc/ppp/ppp%20review/forms/personalview.aspx>
- 2.2 This process provides program offices with a consolidated, repeatable approach to integrate and document PPP and SSE efforts IAW existing DoD, AF and AFLCMC processes. It applies to all acquisition programs and modifications IAW DoDI 5000.02T, *Operation of the Defense Acquisition System*, DODI 5000.02, *Operation of the Adaptive Acquisition Framework*, and AFI 63-101/20-101, *Integrated Life Cycle Management*.
- 2.3 This process also applies to Defense Business Systems (DBS) if designated as a Major Defense Acquisition Program (MDAP) and/or considered an “applicable system” IAW DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. NOTE: DBS will follow the guidance provided in DoDI 5000.75, *Business Systems Requirements and Acquisitions* and AFMAN

63-144, *Defense Business System Life Cycle Management* if not designated as an MDAP or “applicable system”.

- 2.4 This process is required for all Acquisition Category (ACAT) programs beginning at Milestone (MS) A and every subsequent Milestone Decision including Full-Rate Production. IAW AFI 63-101/20-101, *Integrated Life Cycle Management*, at a minimum, review the PPP every five (5) years congruent with Life Cycle Sustainment Plan updates; however, the PPP process shall be reviewed during each System Engineering Technical Review and all major milestone events to assess updates to CPI/CC, security risks, and mitigations with updates recorded in the PPP. The PPP is approved by the Milestone Decision Authority (MDA). An approved PPP is also included as supporting documentation in the attachment section of the Information Support Plan (ISP). For programs with the Defense Acquisition Executive (DAE) as the MDA, refer to USAF Program Protection / Systems Security Engineering Guidebook coordination and approval section. See section 4.1 for more detail on the routing process.
- 2.5 Legacy system or modification programs can satisfy PPP requirements by updating or annexing the existing PPP, or by creating a separate PPP for legacy systems or modification.

3.0 Entry and Exit Criteria for Program Protection Planning

3.1 Entry Criteria

- 3.1.1 A draft PPP (approved by the PM, PEO and Component Acquisition Executive (CAE)/DAE)) is due for the Development RFP decision.
- 3.1.2 The PPP will be submitted for MDA approval at each milestone review, beginning with MS A. For programs with the DAE as the MDA, PPPs will be submitted to the Deputy Assistant Secretary of Defense (Systems Engineering) (DASD(SE)) not less than 45 calendar days prior to the relevant review. Note: IAW with Table 2 in Enclosure 1 of DoDI 5000.02T, *Operation of the Defense Acquisition System*, the DAE may delegate authority to act as the MDA to the head of a DoD Component, who may further delegate the authority to the CAE.
- 3.1.3 Program protection continues throughout the system lifecycle. For MS B, the DoD Component-approved draft PPP will be provided to the DASD(SE) 45 days prior to the Development RFP Release Decision Point. Note: It is recommended to update the PPP for each System Engineering Technical Review (SETR), and as often as required after the updated analyses have been conducted to support submission at milestone decisions.
- 3.1.4 The PPP will be routed to AFLCMC/IP along with all Annexes, and copies of DD Form 254s for review as identified in Table 1 below.
- 3.1.5 PMs will submit the program's Cybersecurity Strategy as an appendix of every PPP.
- 3.1.6 Submit an Anti-Tamper (AT) concept before MS A and AT plans before MS B and MS C; the DoD AT Executive Agent (ATEA) must concur with the concept and plans, and the MDA must approve the concept and plans as an element of the PPP.

3.2 Exit Criteria

- 3.2.1 After the full rate production or full deployment decision, the PPP will transition to the PM responsible for system sustainment and disposal.
 - 3.2.2 The exit criteria for PPP is the decommissioning or disposal of a system. The PPP should have a demilitarization or decommissioning Annex detailing this requirement.
- 3.3 MS and Phase Information Requirements Table 1. (IAW DoDI 5000.02T, *Operation of the Defense Acquisition System*, Table 3).
- 3.4 IAW DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*; PMs will develop an acquisition strategy for MDA approval that matches the acquisition pathway (see Figure 1) processes, reviews, documents, and metrics to the character and risk of the capability being acquired. Refer to DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, paragraphs 4.2 for a detailed explanation of the AAF pathways depicted in Figure 1. Use the links provided at paragraph 4.3 for additional policy and purpose of each pathway.

Table 1: Milestone and Phase Information Requirements

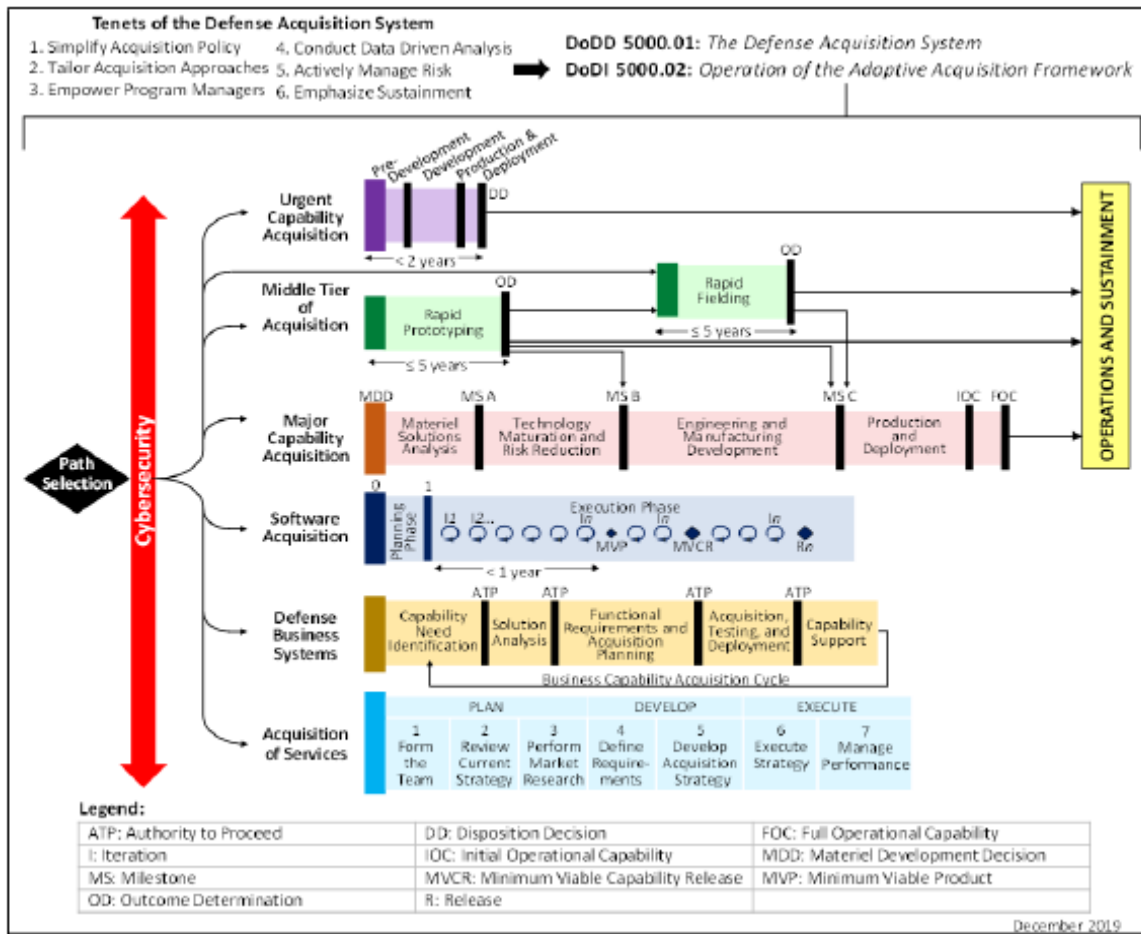
Information Requirement	Program Type ¹				Life-Cycle Event ^{1,2,3}								Source	Approval Authority
	MDAP	MAIS	ACAT		MD	MS	CDD	Dev RFP Rel	MS B	MS C	FRP /FD Dec	Other		
			II	< or = III										
Program Protection Plan (PPP)	X	X	X	X		X		*	*	*	*		DoDI 5200.39 (Ref (ai)) DoDI 5200.44 (Ref (aj)) Para 13a in Enc 3, of DoDI 5200.02T	MDA
Cybersecurity Strategy	X	X	X	X		X		*	*	*	*		SEC 811, PL 106-398 (Ref (q)) 40 USC 11312 (Ref (p)) DoDI 8500.01 (Ref (x))	DoD CIO; Component CIO

Regulatory. A draft⁴ update is due for the Development RFP Release decision and is approved at Milestone B. The PPP includes appropriate appendixes or links to required information. See section 13 in Enclosure 3, of DoDI 5200.02T.

STATUTORY for mission critical or mission essential IT systems. Regulatory for all other programs containing IT, including NSS. See section 6 of Enclosure 11 and Enclosure 13. The CYBERSECURITY STRATEGY is an appendix to the Program Protection Plan (PPP). A draft⁴ update is due for the Development RFP Release and is approved at Milestone B. May include the approved DoD Risk Management Framework Security Plan for urgent needs. The DoD CIO is approval authority for ACAT ID and all ACAT IA programs; the Component CIO is approval authority for all other ACATs.

Table Notes:
 1. An (X) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, an asterisk (*) indicates the requirement for updated information.
 2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
 3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
 4. Requires a Program Manager-, PEO-, and CAE-approved draft.
 5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
 6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 3 requirements associated with that milestone.

Figure 1: Adaptive Acquisition Framework (AAF)



4.0 Program Protection Plan Coordination and Approval

4.1 PPP Coordination and Approval

Table 2: PPP Coordination and Approval

Milestone Decision Authority	Coordination
Defense Acquisition Executive (DAE)	<ol style="list-style-type: none"> 1. Route the draft PPP for review/coordination internally IAW PEO/Directorate requirements. 2. Coordinate an initial/informal review of the PPP with AFLCMC/IP. Load PPP to: https://usaf.dps.mil/sites/21259/aflcmc/ppp/ppp%20review/forms/personalview.aspx for review. 3. Refer to the USAF Weapon System Program Protection / Systems Security Engineering Guidebook, Table 1: PPP Coordination and Approval, for specific routing for the Air Staff, through SAF/AQR and DASD/SE.
Component Acquisition Executive (CAE)	<ol style="list-style-type: none"> 1. Route the draft PPP for review/coordination internally IAW PEO/Directorate requirements. 2. Coordinate an initial/informal review of the PPP with AFLCMC/IP. Load PPP to: https://usaf.dps.mil/sites/21259/aflcmc/ppp/ppp%20review/forms/personalview.aspx for review. 3. Refer to the USAF Weapon System Program Protection / Systems Security Engineering Guidebook, Table 1: PPP Coordination and Approval, for specific routing for the Air Staff through SAF/AQR.
Program Executive Officer (PEO)	<ol style="list-style-type: none"> 1. Route the draft PPP for review/coordination internally IAW PEO/Directorate requirements 2. Coordinate an initial/informal review of the PPP with AFLCMC/IP. Load PPP to: https://usaf.dps.mil/sites/21259/aflcmc/ppp/ppp%20review/forms/personalview.aspx for review. 3. Refer to the USAF Weapon System Program Protection / Systems Security Engineering Guidebook, Table 1: PPP Coordination and Approval, for PEO review and approval.

4.1.1 Route the draft program office PPP to AFLCMC/IP prior to formal PEO signature and external coordination requirements at the link in Table 2. For classified submissions (Secret or Confidential) submit documents to the following link:
https://intelshare.intelink.sgov/sites/ppprepositorysite/_layouts/15/start.aspx#/SitePages/Home.aspx.

4.1.1.1 Contact the ATEA at AFLCMC/XZZ Outreach Workflow: AFLCMC.XZZ@us.af.mil. Ensure classified appendices are not uploaded to unclassified networks or email. Contact the ATEA directly for classified submission processes.

4.1.1.2 For the Supply Chain Risk Management Plan (SCRM) submission, contact the SCRM Network at AFLCMC/LG-LZ SCRM Network Workflow:
AFLCMCLG-LZ.SCRM.Network@us.af.mil.

4.1.2 Submit the Cybersecurity Strategy (CSS) IAW the Clinger-Cohen Act (CCA). Note: the Cyber Test Strategy is a component of the CSS. The CS should also identify test and evaluation boundaries, resources, etc. CS is key element number 9 of the CCA. Note: The CROWS has placed Cyber Focus Teams (CFTs) in each PEO. IAW AFI 63-101/20-101, *Integrated Life Cycle Management*, paragraph 6.10, the PM is responsible for ensuring programs develop and implement a CSS, as

an appendix to the PPP throughout the system life cycle. The CSS is approved by the applicable Chief Information Officer (CIO) prior to MS decisions or contract awards and is required for every MS review beginning at MS A. PMs, System Security Engineers, and Program Protection personnel should use their CFTs members for cybersecurity risk assessment and cybersecurity strategy coordination requirements prior to submission to the CIO.

4.1.3 Provide applicable CRM for external reviews along with the draft PPP submitted to AFLCMC/IP.

4.2 Program offices may communicate directly with AFLCMC/IP (Program Protection Team) via the PPP workflow email inbox: AFLCMC.IPPPP.Workflow@us.af.mil.

5.0 Roles and Responsibilities

- 5.1 Detailed responsibilities for key PPP tasks are found in the USAF Weapon System Program Protection / System Security Engineering Guidebook. The listed roles are IAW AFPAM 63-113, *Program Protection Planning for Life Cycle Management* and the *Defense Acquisition Guidebook*, Chapter 9.

6.0 Tools and Training

- 6.1 Anti-Tamper Website

<https://at.dod.mil/>

- 6.2 Cyber Policy for Cyber Survivability, Test & Evaluation, etc

<https://intelshare.intelink.gov/sites/cybersurvivability/SitePages/Home.aspx>

- 6.3 Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems

<https://www.milsuite.mil/book/docs/DOC-543888>

- 6.4 DoD Cybersecurity Test and Evaluation Guidebook

<https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf>

- 6.5 National Institute of Standards and Technology (NIST) Special Publication Website

<https://search.usa.gov/search?affiliate=nist-search&query=SP&commit=Search>

- 6.6 PM Toolkit

<https://hanscomnet.hanscom.af.mil/pmtb/alpha.html>

- 6.7 Systems Engineering DAU courses

<https://www.dau.edu/training/career-development/engineering>

- 6.8 USAF Combined Process Guide for Critical Program Information (CPI) and Critical Components Identification - Refer to USAF PP/SSE Guidebook, Appendix B

<https://usaf.dps.mil:/w:/r/sites/CROWS/Shared%20Documents/CROWS%20Products/USAF%20Weapon%20System%20PP%20and%20SSE%20Guidebook%20v2.0.docx?d=weea95dad58484c9dace9991ac7e3875e&csf=1&web=1&e=t3wZwd>

- 6.9 USAF SSE Acquisition Guidebook

<https://www.milsuite.mil/book/docs/DOC-668532>

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

- 6.10.1 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>

- 6.10.2 Defense Acquisition University offers a 17-hour ACQ-160 Program Protection Planning Awareness course available here:

<https://icatalog.dau.edu/onlinecatalog/courses.aspx>

7.0 Definitions and Acronyms

- 7.1 Definitions are contained in the USAF Systems Security Engineering Acquisition Guidebook. A link to this document is in Table 3.
- 7.2 Acronyms used in this document are defined in Appendix 2.

8.0 References to Law, Policy, Instructions or Guidance

Table 3: Key References




Number	Title
Acquisition Intelligence Guidebook	Available at: https://www.milsuite.mil/book/docs/DOC-600439
AF CROWS CICC and Cyber IRT for Weapon Systems CONOPS	Air Force CROWS Cyber Incident Coordination Cell (CICC) and Cyber Incident Response Team (IRT) for Weapon Systems Concept of Operations (CONOPS)
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
AFLCMC Standard Process for Cybersecurity Assessment and Authorization	Standard Process for Cybersecurity for all of AFLCMC weapon systems will add to the understanding of cybersecurity in the Air Force and AFLCMC
AFMAN 14-401	Intelligence Analysis and Targeting Tradecraft / Data Standards
AFMAN 17-1402	Air Force Clinger-Cohen Act (CCA) Compliance Guide
AFPAM 63-113	Protection Planning for Life Cycle Management
AFMAN 63-144	Business Capability Requirements, Compliance, and System Acquisition
CNSSI 1253	Security Categorization and Control Selection for National Security Systems
Cyber Survivability Endorsement Implementation Guide v 1.0.1	Joint Chiefs of Staff Cyber Survivability Endorsement Implementation Guide

Number	Title
Defense Acquisition Guidebook Chapters 3, 7 and 9	Chapter 3: Systems Engineering Chapter 7: Intelligence Support & Acquisition Chapter 9: Program Protection
DoDD 5200.47E	Responsibilities for Anti-Tamper (AT) protection of (CPI)
DoDD 5240.24	Counterintelligence Activities Supporting Research, Development, and Acquisition
DoDD 8140.01	Cyberspace Workforce Management
DoDI 5000.01	The Defense Acquisition System
DoDI 5000.02	Operation of the Defense Acquisition System
DoDI 5000.75	Business Systems Requirements and Acquisitions
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
DoDI 8500.01	Cybersecurity
DoDI 8510.01	Risk Management Framework (RMF) for DoD IT
DoDM 5200.45	Instructions for Developing Security Classification Guides
DoD 5220.22-M	National Industrial Security Program Operation Manual
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

Number	Title
USAF Systems Security Engineering Acquisition Guidebook	Available at: https://www.milsuite.mil/book/docs/DOC-668532
USAF Weapon System Program Protection / System Security Engineering Guidebook v2.0	Available at: https://usaf.dps.mil/sites/21259/aflcmc/ppp/ppp%20review/forms/personalview.aspx

APPENDIX 1 – Attachments

The following attachments are useful aides in preparing and executing a Program Protection Plan.

<p>Attachment 1: Office of the Secretary of Defense (OSD) PPP Outline and Guidance</p> 	 <p>OSD PPP Outline and Guidance</p>
<p>Attachment 2: PPP Example</p> 	 <p>FIREBIRD PPP (SAMPLE PPP 2017).d</p>
<p>Attachment 3: OSD Evaluation Criteria</p> 	 <p>OSD PPP Evaluation Criteria</p>
<p>Attachment 4: Cyber War Gaming Document</p> 	 <p>Cyber War Gaming.docx</p>
<p>Attachment 5: Cyber War Gaming Template</p> 	 <p>CWG Template.xlsx</p>
<p>Attachment 6: Cybersecurity Strategy (CSS) Condensed Version (for Non ACAT/BCAT 1) Outline and Guidance</p> 	 <p>Condensed CSS Outline and Guidan</p>
<p>Attachment 7: Cybersecurity Strategy Template</p> 	 <p>Cybersecurity Strategy Template - :</p>
<p>Attachment 8: Change Management Plan</p> 	 <p>PPP_SSE CMP.docx</p>

APPENDIX 2 – Acronym Listing

Acronym	Definition
AAF	Adaptive Acquisition Framework
ACAT	Acquisition Category
AFLCMC	Air Force Life Cycle Management Center
AT	Anti-Tamper
ATEA	Anti-Tamper Executive Agent
CAE	Component Acquisition Executive
CC	Critical Components
CCA	Clinger-Cohen Act
CFT	Cyber Focus Team
CICC	Cyber Incident Coordination Cell
CIO	Chief Information Officer
CONOPS	Concept of Operations
CPI	Critical Program Information
CRM	Comments Resolution Matrix
CROWS	Cyber Resiliency Office for Weapon Systems
CSS	Cybersecurity Strategy
DAE	Defense Acquisition Executive
DAU	Defense Acquisition University
DASD(SE)	Deputy Assistant Secretary of Defense for Systems Engineering
DBS	Defense Business Systems
IAW	In Accordance With
IP	Information Protection
ISP	Information Support Plan
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MS	Milestone
NIST	National Institute of Standards and Technology
OSD	Office of the Secretary of Defense
PEO	Program Executive Officer
PM	Program Manager
PPP	Program Protection Plan or Planning (within context or section)
RFP	Request for Proposal
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SE	Systems Engineering
SETR	Systems Engineering Technical Review
SSE	Systems Security Engineering
TSN	Trusted Systems and Networks
WBS	Work Breakdown Structure

