TABLE OF CONTENTS

CHAPTER 1 ACQUISITON SECURITY MODULE BUSINESS RULES

1 Purpose and Overview

The purpose of this section is to define the Acquisition Security Module (ASM) business rules for roles and responsibilities, functions, maintenance, and administration of the ASM hierarchy.

Business rules are established to provide clarity to the Acquisition community with regard to roles and responsibilities of personnel using the ASM tool. These business rules codify responsibilities for users and for administering the hierarchy, which determines the data accessible to users. It also provides guidance on access to, and use of, the unclassified training site and formalizes a naming convention for assessments. These business rules will (1) allow services and agencies to manage their users and hierarchy and (2) facilitate the association of assessment data for source selection and contract award processes.

Failure to follow the business rules may result in loss of ASM user rights and privileges. Reinstatement will be on a case-by-case basis.

The ASM, a subset of the Enterprise Protection Risk Management (EPRM) platform, is a web-based, cross-disciplinary decision support tool for security compliance and risk assessments. The tool facilitates and standardizes processes and promotes early implementation of cost-effective countermeasures. The Air Force Cyber Resiliency Office for Weapon Systems (CROWS) funded the development of this module.

Protection of Controlled Unclassified Information (CUI), Controlled Technical Information (CTI), and Critical Program Information (CPI) is crucial to building a resilient weapon system. The Acquisition Community has pockets of security excellence throughout the acquisition enterprise to protect CUI, CTI, and CPI. The community does not have sustainable, repeatable, processes based on objective assessments used to evaluate countermeasure effectiveness. The ASM serves to bridge that gap; automate/aid in the development of contract language to address traditional security concerns; integrate threats into countermeasure selection; manage risk activities at the appropriate owner/level; reduce data mining efforts; and leverage and apply traditional security requirements generated from key stakeholders.

The ASM:

- Generates traditional countermeasures using standardized and automated methodology
- **Objectively** evaluates countermeasure effectiveness
- Produces quantifiable data for Acquisition Security Specialists, Engineers, Program Managers, and Industry Partners
- Supports risk-based decision making throughout the acquisition life cycle

2 ASM Administrative Roles and Responsibilities Reference Table

The purpose of this section is to define the Acquisition Security Module (ASM) business rules for administrative roles and responsibilities, functions, maintenance, and administration of the ASM hierarchy.

ROLE	RESPONSIBILTIES	PROPOSED May be assigned the following ASM Roles
The Office of the Assistant Secretary of the Air Force for Security, Counter Intelligence & Special Programs (SAF/AAZ)	• Overall EPRM program management to include budgeting and Program Objective Memoranda for EPRM resources • Establishes Configuration Control Boards to vet and prioritize requirements and codify EPRM policy ○ Administers policy for EPRM ○ Ensures ASM process is being followed in accordance with EPRM business rules • Provides training for EPRM administrators and assessment managers • Provides helpdesk support to administrators • Solicits feedback for ASM tool updates and communication • Provides helpdesk support to administrators ○ EPRMhelp@alionscience.com (Unclassified) ○ http://EPRMhelp.countermeasures.com/ ○ 1 (800) 754-4204 (0800-1700 Eastern)	• Reviewer (Read Only)
PROGRAM MANAGER, ASM (SAF/AQR)	• Ensures ASM process is being followed • Contributes to overall ASM program management to include budgeting and Program Objective Memoranda for EPRM resources • Works in conjunction with SAF/AAZ on modifications to ASM • Oversees ASM process including: ○ Account approval for Major Command and Direct Reporting Unit administrators ○ Training via Defense Connect Online for Enterprise Protection Risk Management administrators and assessment managers ○ Briefs CROWS leadership on ASM metrics • Forms and oversees ASM working groups as need to update tool • Approves user request forms prior to submittal to EPRM helpdesk • Oversees administrative functions including: ○ Changes in nodal hierarchy ○ Update of asset templates ○ Update of threat templates • Update of training material	• Reviewer (Read Only)

ROLE	RESPONSIBILTIES	PROPOSED May be assigned the following ASM Roles
CROWS CONFIGURATION CONTROL BOARD (CCB)	• Modify and update the ASM tool for applicability to current programs when needed • Maintain proficiency on the ASM tool • Review ASM organizational structure • Ensure ASM process is being followed • Works in conjunction with SAF/AAZ on modifications to ASM • Develop user training for use of the ASM module • Develop countermeasure/threat databases for templates • Creates templates • May copy from previous assessments and templates • “Expires” templates to remove accessibility from users • Make modifications to templates	• Reviewer (Read Only) • Templator • Template Manager
PROGRAM EXECUTIVE OFFICERS (PEOs)	• Ensure PMOs correctly utilize ASM as part of the Acquisition Security process • Ensure PMOs implement ASM in concert with Acquisition Security activities • Review assessments and reports within their programs • Ensure PMO users get adequate training for use of the ASM module • May delegate node administration, but will limit their privileges to their hierarchy • Cannot elevate any user privileges outside their portion of the hierarchy • Adjust countermeasure/threat data from inherited template(s)	• Reviewer (Read Only) • Assessment Manager • User Admin
PROGRAM MANAGEMENT OFFICES (PMOs)	• Modify and update the ASM tool for applicability to current programs when needed • Brief leadership on ASM capabilities • Receive and approve/deny user requests for access to ASM • Review assessment and reports within their programs • Establish ASM organizational structure • Update nodes within their program • Maintain proficiency on the ASM tool • Oversee security working groups on ASM Management processes and results • Assist leadership with establishing ASM business rules (when applicable) • Assign/share their assessments within their purview • Conduct initial assessments on new, developing, or modified programs	• Assessor • Assessment Manager • Node Admin • Templator (in conjunction with CCB)

Figure 1: ASM Administrative Roles and Responsibilities Table

3 ASM User Roles and Privileges Definition Table

The purpose of this section is to define user roles and functions for the ASM.

Personnel may be assigned multiple roles and are responsible for their hierarchy in the ASM.

ROLE	RESPONSIBILTIES/CONSTRAINTS
REVIEWER (READ ONLY) (SAFHHQ/CCB/PEO/PMO	• Can view all assessments within assigned hierarchy • Can print reports • Does not have any edit capability
TEMPLATE MANAGER (CCB)	• Can expire templates
TEMPLATOR (CCB and PMO)	• Can create templates • Can expire templates
USER ADMINISTRATOR (PEO LEVEL)	• Can see the global list of users • Edit user contact information for any user • Remove users from the global list and assign/remove user privileges at one or more nodes within their area of the hierarchy • Assign user and hierarchy administrator privileges within their hierarchy and below • Can create new users; however, primary responsibility for user management is the EPRM Help Desk • Provide the Help Desk with a names to update user rosters and email lists • Shall not create other User Administrators, request through EPRM Help Desk • Shall not expire users; request in an email to EPRM Help Desk
HIERARCHY (NODE) ADMINISTRATOR	• Create new nodes for installations/units/etc. within the user's hierarchy, i.e., below the node at which the user is assigned • Edit node names at or below their hierarchy • Move nodes within their users' hierarchy • Make changes to hierarchy when requested by the Assessment Manager • Cannot delete Nodes due to cascading effects; however may request deletion of a Node through the EPRM Help Desk • Cannot edit names of their top-level node or move units outside of their hierarchy; however, may request changes through the EPRM Help Desk

ROLE	RESPONSIBILTIES/CONSTRAINTS
ASSESSMENT MANAGER PEO/PMO	• View and update new risk-based assessment data including results/observations/ findings, etc. • Edit assessment name(s) to ensure consistency • Able to view data for all programs they have responsibility for • Role may be delegated to subordinate echelons and functional components by the AQ component, within their hierarchy (but not above their hierarchy) • May delegate this role to their AQ Component • Coordinates with the assessment owner and EPRM Help Desk • May delete assessments • May not edit assessments; however, may reject assessments with sufficient justification
ASSESSORS (PMO)	• Scope their program in ASM and complete assessments for their PMO • May be anyone who has user responsibilities to complete assessments • Uses templates associated with their level in the hierarchy and below • Create assessments using “inherit” from one or more previously created templates • Copy from previous assessments • Analyze assessments • Prints reports • Submit completed assessments • May be assigned multiple roles within ASM such as Templator, Assessment Manager, and Node Administrator • Update countermeasure selection as determined by their IPTs/PMO • Update countermeasures received from prospective & contracted industry partners • Update contract numbers, cage codes, & contractor locations for their programs • Produce analytical products from ASM for PM & PEO risk acceptance • Conduct Program Protection assessments within ASM • Build the Dashboard for their PM and PEO • Uploads PPP artifacts

Figure 2: ASM User Roles and Privileges Table

4 ASM Role Privileges

The table below shows the privileges for each role in ASM. A user may be assigned multiple roles.

	FUNCTONS															
Role	Use Templates within assigned area(s)	Create Templates within assigned area(s)	View Templates (not owned by the user) within assigned area(s)	Expire Templates within assigned area(s)	Create Assessments and Surveys within assigned area(s)	View Assessments and Surveys (not owned by the user) within assigned area(s)	Assign (transfer ownership of) assessments and surveys within assigned area(s)	Share assessments and surveys within assigned area(s)	Edit Locked assessments and surveys within assigned area(s)	Print Reports within assigned area(s)	Delete Assessments and Surveys within assigned area(s)	Add Nodes within assigned area(s)	Edit/Move Nodes within assigned area(s)	View Users within assigned area(s)	Edit/Add/ Remove user privileges within assigned area(s)	View References
Assessor	X				X		X*	X*	X*	X*	X*					X
Assessment Manager						X	X	X	X	X	X					X
Templator		X		X*												X
Template Manager			X	X												X
Node Admin			X$			X$						X	X	X$		X
User Admin														X	X	X
Reviewer						X				X						X

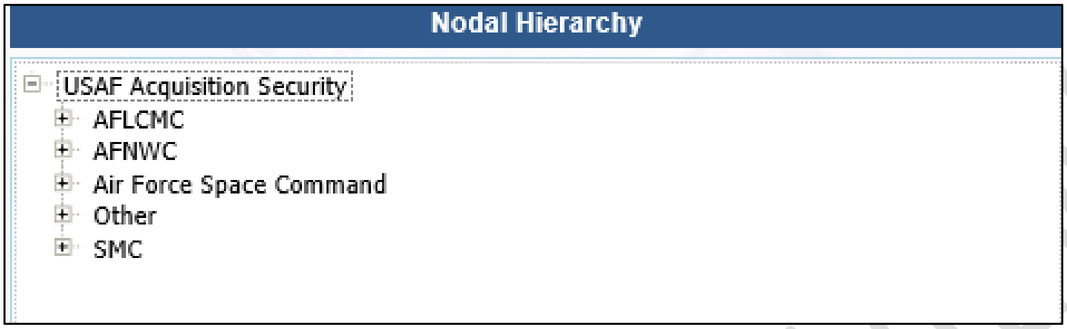
* Assessor/Templator only grants privilege to create assessment/template owned by that user. Once user owns an assessment/template, ability to manipulate is granted via ownership rather

$ Node Admin can see (1) list of users with any role/cap node at or above selected node; (2) list of assessments and surveys at or below selected node; and (3) list of templates at or above selected node, when a node is selected on the Node Admin page. Node Admin cannot open any such user profile, assessment, survey or template and view its details.

Figure 3: ASM Administrative Roles and Functions

5 Hierarchy/Nodes

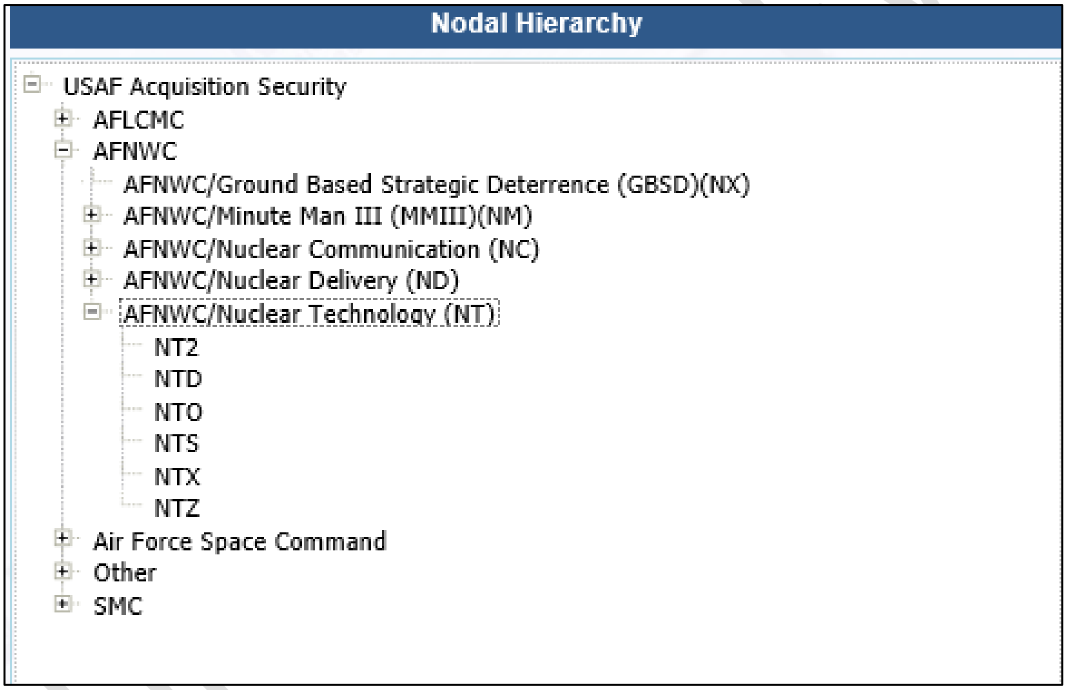
The ASM is located under the DoD – USAF Acquisition Security hierarchy in EPRM. The ASM nodal hierarchy mirrors the organization of the Acquisition Security program starting with Centers then by Directorates then by programs. The figures below show how the hierarchy is set up.



Nodal Hierarchy

- USAF Acquisition Security
  - AFLCMC
  - AFNWC
  - Air Force Space Command
  - Other
  - SMC

Figure 4: ASM nodal hierarchy (unexpanded)



Nodal Hierarchy

- USAF Acquisition Security
  - AFLCMC
  - AFNWC
    - AFNWC/Ground Based Strategic Deterrence (GBSD)(NX)
    - AFNWC/Minute Man III (MMIII)(NM)
    - AFNWC/Nuclear Communication (NC)
    - AFNWC/Nuclear Delivery (ND)
    - AFNWC/Nuclear Technology (NT)
      - NT2
      - NTD
      - NTO
      - NTS
      - NTX
      - NTZ
  - Air Force Space Command
  - Other
  - SMC

Figure 5: Example of expanded hierarchy

Adding/Removing Nodes

- If a node addition or removal is required, a request from the Center level will be sent to ERPMhelp@alionscience.com with the following information:
  - Program Executive Office (PEO):
  - Program Management Office (PMO):
  - Node (Program) Name:
- This request can take up to 48 hours to complete.

6 Adding New Users

The full ASM tool (classified) resides on SIPRNet. You must have a SIPRnet account to gain access. If you do not have a SIPRnet account, you can use the demo version (unclassified) of the tool. **Go to Chapter2, section 5 to view demo instructions.**

Users are added at the level of their corresponding nodal hierarchy (level within the organization). Users are able to see everything in their node and anything below their node.

Users can request a login directly through the EPRM tool by clicking on the Request User Profile on the login screen or by forwarding the following information to the EPRM Help Desk at EPRM Help Desk.

Login requests are forwarded to the Approving Official by the Alion EPRM Help desk.

For roles other than assessor or assessment manager, additional approvals are required.

When submitting the request, users are added to both the SIPRNet ASM (providing you have a SIPR account) and the demo version of ASM. This process may take up to 48 hours.

Name:				
Title/ Rank:				
Phone number:				
Service or Component:	**Air Force**			
Center (i.e., AFLNWC)				
Two letter Directorate (i.e., ND)				
Three letter Program (i.e., ND1)				
Program Executive Officer (PEO)				
Alion Contract Name:	**Acquisition Security**			
NIPR E-Mail:				
SIPR E-Mail:				
THE FOLLOWING INFORMATION WILL BE COMPLETED BY APPROVING OFFICIAL AND THE EPRM HELP DESK				
Node Assignment	Center level (TWO DIGIT)	Dictorate level (THREE DIGIT)		
(Add "X" next to applicable level)				
Role(s)	Assessor	Assessment Mgr		
(Add "X" next to applicable level)				
The following roles require additional approval				
Templator	Template Mgr	Node Admin	User Admin	Observer

Figure 6: Login request form

7 ASM Assessment Naming

ASM assessment names are automatically added as the assessment is completed. The following syntax is used to name assessments:

Objective – Date started – Three letter Program – Program Name – Type of Assessment -CAGE code of Prime – Who provided Information – Name of Subcontractor (if applicable)

Here are some examples:

- ASM – 07/10/2020 - WWL - FIREBIRD - SOURCE SELECTION - 1651651615 – PRIME
- ASM – 07/30/2020 - WWL – FIREBIRD – CONTRACT AWARD – 1651651615 - SUBCONTRACTOR-ABC

Name	Indicates	Used when:
ASM – 07102020 - WWL - FIREBIRD – BASELINE-No Cage Code- Program Office	**Baseline assessment** of WWL program "Firebird" created 7 July 2020 by the Program Office. Since a prime has not yet been identified, the assessment name indicates "No Cage code".	Creating the initial program assessment.
ASM – 07302020 - WWL - FIREBIRD – PM Approved RFP-No Cage Code- Program Office	**PM Approved RFP assessment** created 30 July 2020 for the WWL Firebird program showing acceptable risk created by Program Office.	Creating an assessment defining the requirements for inclusion in the RFP package. Countermeasures answered "yes" in this assessment will be included in the Statement of Work (SOW).
ASM – 08312020 - WWL - FIREBIRD – Source Selection - 54876 - Prime	**Source Selection** assessment created 31 August 2020 for the WWL program reflecting the answers the Prime (Cage code 54876) provided in the RFP response.	Creating an assessment using the answers provided by the offeror(s).
ASM – 09012020 - WWL - FIREBIRD – Contract Award -54876 – Prime – Sub – ABC Company	**Contract Award** assessment created 01 September 2020 for the WWL Firebird program reflecting information provided by the sub (ABC Company) of the Prime (Cage code 54876).	Creating an assessment to ensure security requirements are flowed to the subs. Every sub of the Prime should be completing an assessment.
ASM – 09222020 - WWL - FIREBIRD – Milestone Update - 54876 – Program Office	**Milestone Update** assessment created 22 September 2020 for the WWL Firebird program reflecting risk at a milestone update with answers provided by the Program Office	Creating an assessment for a milestone update (threat change, contract change). This can be done for a Prime, sub or PM Office.
ASM – 10022020 - WWL - FIREBIRD – Sustainment - 54876 - Prime	**Sustainment** assessment created 02 October 2020 for the WWL program reflecting the risk at a periodic update with answers provided by the Prime.	Creating a periodic assessment using data provided by the Prime. This can also be done by the Program Office for the PMO assessment.

Figure 7: Examples of ASM assessment naming conventions

8 Program Protection Plan (PPP)

Overview

Program protection is a critical element of the Integrated Life Cycle Management (ILCM) of weapon systems and services. The Program Protection Plan (PPP) documents program decisions to ensure that technology, components, and information are adequately protected.

Purpose

The program must meet DoD and AF regulatory requirements and follow the USAF Weapons System PPP/SSE guidebook. In addition to SCG requirements, there are 22 regulatory requirements for PPP sufficiency. The Program Office identified PPP “completed” areas and the status for unmet requirements. Not all of these regulatory requirements are calculated into the overall program risk or protection suitability score. Those marked with an asterisk (*) are part of the overall risk score.

Documentation/File Upload

PPP documentation and associated files can be added directly into ASM using upload file functionality.

Files are uploaded on the Program Protection Plan home page using the file upload button. Files to upload include the following:

Area	Relative PPP Question	Required Documentation
Signed PPP	1. Has a PPP been developed and approved for ALL programs beginning at MS A and every subsequent Milestone Decision including Full-Rate Production, and approved by the MDA? (Note: The annex is effectively a “stand alone” PPP for the modification/upgrade effort) Reference: AFI 63-101/20-101	Approved PPP
Criticality Analysis (CA), SCRM & TSN	6. Did the program request and/or receive an Integrated Threat Assessment (ITA) from AFOSI and a DIA Threat Analysis Center (DIA TAC) Supply Chain Threat Assessment to assess threats posed to CPI (ITA) and Critical Components (DIA TAC)? Reference: AFI 63-101/20-101	ITA and DIA TAC
Intelligence Support	7. Has the program completed a Counterintelligence Support Plan (CISP) with the supporting AFOSI unit to ensure counter-intel support is provided for the program? Reference: AFI 63-101/20-101	CISP with supporting AFOSI

Area	Relative PPP Question	Required Documentation
Critical Program Information (CPI) & Anti-Tamper (AT)	18. Did the program determine requirements, plan, design, implement, test, and evaluate AT based on the consequence of CPI compromise and the anticipated system exposure and in alignment with requirements guidance from the DoD Executive Agent for AT (SAF/AQL)? Reference: DoDD 5200.47E, September 4, 2015 Anti-Tamper (AT)	CPI and AT Plan
Contract Language	19. Did the program identify OPSEC requirements on the DD Form 254, contracts and SOW/PWSs with sufficient detail to ensure contractor understanding of the exact OPSEC provisions or measures required by the organization? (Note OPSEC requirements should be program specific, and not refer to base or local OPSEC plan). Reference: AFI 10-701, Operations Security Program	OPSEC Requirements

Figure 8: Required Program Protection Plan (PPP) documents

Reporting

Program Protection is reported in the ASM Executive Summary Report and in the ASM Dashboard report. For all items, those fully completed will show in green on the reports those not completed or scheduled will show as red. Items scheduled but not fully complete will show as yellow.

In the Dashboard report, PPP shows as red or green with future functionality showing scheduled as yellow.

The first three questions are taken from the risk assessment of the Program Management Office. These are answered either “Yes” or “No”. The nineteen remaining questions are compliance only. The answers can be “yes”, “no” or “scheduled”.

PPPs are associated with the PMO assessment.

In order for reporting to be complete and accurate, all PPP questions must be answered and the PPP finished and locked. In the event this does not occur, unanswered questions will populate as “PPP not complete”.

The PPP requirements for compliance are shown on the following page.

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
SCG*	Is a Program Security Classification Guide (SCG) identified in the RFP/SOW/SOO and required on the DD Form 254? Reference(s): DODM 5220.22, Volume 2, Paragraph 6.3, a,b, 1 August 2018	*Automatically populated with from assessment*	N/A	N/A	N/A	*Automatically populated from assessment*
Cyber SCG*	Is the AF Cybersecurity SCG (Cyber Security Classification/Declassification Guide for Air Force Weapon Systems) identified in the RFP/SOW/SOO and required on the DD Form 254? Reference(s): DODM 5220.22, Volume 2, Paragraph 6.3, a,b, 1 August 2018	*Automatically populated with from assessment*	N/A	N/A	N/A	*Automatically populated from assessment*
Anti-Tamper SCG*	Is the Anti-Tamper SCG identified in the RFP/SOW/SOO and required on the DD Form 254? Reference(s): DODM 5220.22, Volume 2, Paragraph 6.3, a,b, 1 August 2018; NIST Special Publication 800-53 Revision 4, Appendix F (PE-3(5); SA-10(3); SA-18), 22 January 2015; NIST Special Publication 800-53A Revision 4, Appendix F (PE-3(5); SA-10(3); SA-18), 18 December 2014.	*Automatically populated with from assessment*	N/A	N/A	N/A	*Automatically populated from assessment*
Signed PPP	1. Has a PPP been developed and approved for ALL programs beginning at MS A and every subsequent Milestone Decision including Full-Rate Production, and approved by the MDA? (Note: The annex is effectively a “stand alone” PPP for the modification/upgrade effort) Reference: AFI 63-101/20-101	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP once uploaded*	*Automatically populated from PPP*

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Signed PPP	1a. Have system modifications or upgrades been addressed in the PPP? For legacy systems, PPP requirements for modifications can be satisfied by updating or annexing an existing PPP, creating a separate PPP for each modification, or creating a new PPP for the entire weapon system addressing all modification protection measures with provisions for annexes to cover future modifications. Reference: AFI 63-101/20-101	*Automatically populated from PPP*	N/A	N/A	N/A	*Automatically populated from PPP*
Critical Program Information (CPI) & Anti-Tamper (AT)	2. Did the PM collaborate with the USAF AT Service Lead for Anti-Tamper Planning? Note: SAF/AQL is the Air Force AT Service Lead Reference: AFI 63-101/20-101	*Automatically populated from PPP*	N/A	N/A	N/A	*Automatically populated from PPP*
Criticality Analysis (CA), SCRM & TSN	3. Did the PM identify and maintain an updated list of critical components in the PPP vulnerable to counterfeiting throughout the system life cycle? Reference: AFI 63-101/20-101	*Automatically populated from PPP*	N/A	N/A	N/A	*Automatically populated from PPP*
Contract Language	4. Did the PM ensure contracts require prime contractors take the steps necessary to implement management controls to guard against counterfeit materiel in the supply chain? Reference: AFI 63-101/20-101	*Automatically populated from PPP*	N/A	N/A	N/A	*Automatically populated from PPP*
Software Assurance (SwA)	5. Did the PM ensure Software Assurance (SwA) principles are integrated into the program protection processes of the program and documented in the PPP? Reference: AFI 63-101/20-101	*Automatically populated from PPP*	N/A	N/A	N/A	*Automatically populated from PPP*

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Software Assurance (SwA)	5a. Is SwA implemented as part of software engineering processes and support Cybersecurity requirements applicable to the program? Reference: AFI 63-101/20-101	*Automatically populated from PPP*	N/A	N/A	N/A	*Automatically populated from PPP*
Criticality Analysis (CA), SCRM & TSN	6. Did the program request and/or receive an Integrated Threat Assessment (ITA) from AFOSI and a DIA Threat Analysis Center (DIA TAC) Supply Chain Threat Assessment to assess threats posed to CPI (ITA) and Critical Components (DIA TAC)? Reference: AFI 63-101/20-101	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP once uploaded*	*Automatically populated from PPP*
Intelligence Support	7. Has the program completed a Counterintelligence Support Plan (CISP) with the supporting AFOSI unit to ensure counter-intel support is provided for the program? Reference: AFI 63-101/20-101	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP once uploaded*	*Automatically populated from PPP*
Critical Program Information (CPI) & Anti-Tamper (AT)	8. Was the system assessed for CPI, and reassessed throughout the program's lifecycle so that CPI protections requirements and countermeasures may be identified and applied as the CPI is developed and modified throughout the lifecycle as needed? Reference: DoDI 5200.39, May 28, 2015 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)	*Automatically populated from PPP*	N/A	N/A	N/A	

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Critical Program Information (CPI) & Anti-Tamper (AT)	9. Was CPI horizontally identified and protected to ensure equivalent protections are consistently and efficiently applied across programs based on the exposure of the system, consequence of CPI compromise, and assessed threats? Reference: DoDI 5200.39, May 28, 2015 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)	*Automatically populated from PPP*	N/A	N/A	N/A	
Critical Program Information (CPI) & Anti-Tamper (AT)	10. Do CPI protections include, at a minimum: anti-tamper (as required), security (cybersecurity, industrial security, information security, operations security, personnel security, and physical security), or equivalent countermeasures? Reference: DoDI 5200.39, May 28, 2015 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)	*Automatically populated from PPP*	N/A	N/A	N/A	

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Critical Program Information (CPI) & Anti-Tamper (AT)	11. Did the program use the Acquisition Security Database (ASDB) when conducting horizontal identification and protection analysis of other similar systems? ** Reference: DoDI 5200.39, May 28, 2015 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)	*Automatically populated from PPP*	N/A	N/A	N/A	
Critical Program Information (CPI) & Anti-Tamper (AT)	12. Was program information entered into ASDB, to include inherited and organic CPI? (Note ASDB is accessed through DTIC and is often not accessible. Attempt to access ASDB, if unsuccessful, indicate so in PPP and address how the program contacted similar programs (i.e., contacted similar NAVY program). Reference: DoDI 5200.39, May 28, 2015 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)	*Automatically populated from PPP*	N/A	N/A	N/A	

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Contract Language	13. Did PM include the PPP in RFPs, and prepare updates to the PPP after any contract award to reflect the contractor's approved technical approach and the details or necessary changes that were not available or appropriate prior to contract award? Reference: DoDI 5000.02, January 7, 2015 Operation of the Defense Acquisition System	*Automatically populated from PPP*	N/A	N/A	N/A	
Signed PPP	14. Does the PPP clearly describe the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; the plan to apply countermeasures to mitigate associated risks; and planning for exportability and potential foreign involvement as applicable? Reference: DoDI 5000.02, January 7, 2015 Operation of the Defense Acquisition System	*Automatically populated from PPP*	N/A	N/A	N/A	

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Criticality Analysis (CA), SCRM & TSN	15. Was a criticality analysis completed to identify mission critical functions and critical components to reduce the vulnerability of such functions and components through secure system design? Reference: DoDI 5200.44, November 5, 2012 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)	*Automatically populated from PPP*	N/A	N/A	N/A	
Criticality Analysis (CA), SCRM & TSN	16. Did the program request a DIA threat analysis of suppliers of critical components from the pertinent TSN focal point? Reference: DoDI 5200.44, November 5, 2012 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)	*Automatically populated from PPP*	*Automatically populated from PPP*	N/A	N/A	
Criticality Analysis (CA), SCRM & TSN	17. Does the PPP include the identification of mission critical functions and critical components as well as TSN planning and implementation activities, including risk acceptance as appropriate? Reference: DoDI 5200.44, November 5, 2012 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)	*Automatically populated from PPP*	N/A	N/A	N/A	

Area	Compliance	Complete	Date Approved	Date Due	Required Documentation submitted?	Remarks
Critical Program Information (CPI) & Anti-Tamper (AT)	18. Did the program determine requirements, plan, design, implement, test, and evaluate AT based on the consequence of CPI compromise and the anticipated system exposure and in alignment with requirements guidance from the DoD Executive Agent for AT (SAF/AQL)? Reference: DoDD 5200.47E, September 4, 2015 Anti-Tamper (AT)	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP once uploaded*	
Contract Language	19. Did the program identify OPSEC requirements on the DD Form 254, contracts and SOW/PWSs with sufficient detail to ensure contractor understanding of the exact OPSEC provisions or measures required by the organization? (Note OPSEC requirements should be program specific, and not refer to base or local OPSEC plan). Reference: AFI 10-701, Operations Security Program	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP*	*Automatically populated from PPP once uploaded*	

Figure 9: Program Protection Plan (PPP) reporting matrix

Index of Figures and Images

References

References
AF Pamphlet 63-113, Program Protection Planning for Life Cycle Management, 17 October 2013
Deputy Assistant Secretary of Defense (DASD) Systems Engineering (SE) Program Protection Plan (PPP) Outline and Guidance, Version 1.0, July 2011
Defense Acquisition Guidebook (DAG)
DFARS 252.204-7000 Disclosure of Information. October 2016
DFARS 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls. October 2016
DFARS 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. Oct 2016
DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. October 2016
DFARS 252.208-7400 Enterprise Software Agreements, August 2020
DFARS 252.209-7002 Disclosure of Ownership or Control by a Foreign Government. June 2010
DFARS 252.211-7003 Item Unique Identification and Valuation. March 2016
DFARS 252.225-7048 Export-Controlled Items. June 2013
DFARS 252.225-7049 Prohibition on Acquisition of Certain Foreign Commercial Satellite Services/Representations. December 2018
DFARS 252.227-7013 Rights in Technical Data--Noncommercial Items. February 2014
DFARS 252.239-7000 Protection Against Compromising Emanations. June 2004
DFARS 252.239?7001 Information Assurance Contractor Training and Certification. January 2008
DFARS 252.239-7017 Notice of Supply Chain Risk. February 2019
DFARS 252.239-7018 Supply Chain Risk. February 2019
DFARS 252.246-7003 Notification of Potential Safety Issues. June 2013
DFARS 252.246?7007 Contractor Counterfeit Electronic Part Detection and Avoidance System. August 2016
DoD Directive 5000.39, ACQUISITION AND MANAGEMENT OF INTEGRATED LOGISTIC SUPPORT FOR SYSTEMS AND EQUIPMENT, 17 November 1983

References
DODD 5205.02, DoD Operations Security (OPSEC) Program, 6 March 2006
DoDI 5000.02, Operation of the Defense Acquisition System, 7 January 2015, incorporating Change 3, 10 August 2017
DODI 5200.02, DoD Personnel Security Program (PSP), 21 March 2014
DoD Instruction 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), 28 May 2015, Incorporating Change 2, Effective 15 October 2018
DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), 5 November 2012, Incorporating Change 3, October 15, 2018
DoD Instruction 5230.24, Distribution Statements on Technical Documents, 23 August 2012, Incorporating Change 3, 15 October 2018
DOD 5230.29, Security and Policy Review of DoD Information for Public Release, 13 August 2014, Incorporating Change 1, April 14, 2017
DoD Manual 5200.01, Volume 3, Enclosure 3, DoD Information Security Program: Protection of Classified Information, Paragraph 4, 24 February 2012, Incorporating Change 2, 19 March 2013
DOD 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI), Enclosure 3, 24 Feb 2012, Incorporating Change 1, Effective May 9, 2018
DODM 5220.02, Procedures for the DoD Personnel Security Program (PSP), 3 November 2008, Incorporating Change 1, 26 April 2018
DODM 5220.22, Volume 2, National Industrial Security Program: Industrial Security Procedures for Government Activities, 1 August 2018
Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative
National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI), 17 April 2014.
National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, 28 February 2006, Incorporating Change 2, May 18, 2016
NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015
NIST Special Publication 800-171 Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016

References
NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix F, April 2013, including updates as of 22 January 2015
NIST Special Publication 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Appendix F, 18 December 2014
USAF Systems Security Engineering (SSE) Acquisition Guidebook, 08 May 2018, VERSION 1.3
USDI Memo: Directive-type Memorandum (DTM) 15-002, Policy Guidance for the Processing of National Interest Determinations (NIDs) in Connection with Foreign Ownership, Control, or Influence (FOCI)? 11 February 2015, incorporating change 3, 20 October 2017