PROGRAM NAME – ACAT LEVEL

PROGRAM PROTECTION PLAN

VERSION #

SUPPORTING MILESTONE MS AND

APPROPRIATE PHASE NAME

DATE

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Undersecretary of Defense Date

Acquisition, Technology, and Logistics

[or appropriate Milestone Decision Authority for non-ACAT 1D programs]

DISTRIBUTION STATEMENT Click here to enter distribution letter and explanation (e.g.; “Approved for public release; distribution is unlimited”). Reference <http://www.dtic.mil/dtic/submit/guidance/distribstatement.html> .

SUBMITTED BY

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name Date

Program Manager

CONCURRENCE

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name Date

Program Executive Officer or

Equivalent

COMPONENT APPROVAL

[Required for programs with OSD approval (ACAT 1D, IAM, etc.)]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name Date

Component Acquisition Executive

**Guidance:**

• The purpose of the PPP is to help programs ensure that they adequately protect their technology, components, and information. This includes information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to clone, counter, or defeat war fighting capability.

• The PPP, once in place, should guide program office security measures and be updated as threats and vulnerabilities change or are better understood.

• It is important that an end-to-end system view be taken when developing and executing the PPP. External, interdependent, or government furnished components that may be outside a program managers' control must be considered.

• The PPP is a plan, not a treatise. The PPP should therefore contain information someone working on the program needs to carry out his or her Program Protection responsibilities, and should be generated as part of the program planning process.

• It is possible that not all Program Protection information will be available at Milestone A. Complete the tables/sections with the information available and document the plan to update this information as more details become available. At minimum, a Milestone A PPP should include an initial criticality analysis, candidate CPI, potential countermeasures, and the Information Assurance Strategy. The Milestone B PPP should be a comprehensive document.

• Wherever possible, reference or point to other documents containing relevant information rather than duplicating the information in the PPP, unless that information would be valuable to users of the plan. Do not simply repeat general policies unless that information would be valuable to the user of the plan.

• Appendices are required where relevant and appropriate. For example, every acquisition program must have an Information Assurance Strategy, but not all acquisition programs will have an Anti-Tamper plan.

Determine whether FOUO is applicable per DoDM 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” February 24, 2012.

**Guidance Source**: <http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf>.

The 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 program may opt to reference some tables (e.g. threats, vulnerabilities) as classified appendices.

**Instructions:** PEO-specific instruction to be added.

**References:**

Program Protection Plan Outline and Guidance, Version 1.0, July 2011

[Memorandum for Secretaries of the Military Departments Directors of the Defense Agencies, Document Streamlining – Program Protection Plan (PPP), July 18, 2011](https://dap.dau.mil/policy/Lists/Policy%20Documents/Attachments/3298/USA003781-11_Signed.pdf)

Contents

[1. Introduction – Purpose and Update Plan. 8](#_Toc349042633)

[1.0.1 Users of PPP. 8](#_Toc349042634)

[1.0.2 Alignment with Contractor’s Program Protection Implementation Plan(s) (PPIP). 8](#_Toc349042635)

[1.0.3 Contractor’s Responsibility for Program Protection. 8](#_Toc349042636)

[1.0.4 Timing of and Criteria for PPP updates. 8](#_Toc349042637)

[1.0.5 Update Authority. 8](#_Toc349042638)

[1.0.6 Approval Authority for Different Updates. 8](#_Toc349042639)

[1.0.7 PPP Update Record. 8](#_Toc349042640)

[1.1. Technology/System Description. 9](#_Toc349042641)

[1.1.1. Link to Reference Document. 9](#_Toc349042642)

[1.1.2. Program Information. 9](#_Toc349042643)

[1.2. Program Protection Responsibilities. 9](#_Toc349042644)

[1.2.01 Countermeasure Execution Responsibility. 10](#_Toc349042645)

[1.2.02 Program Protection Responsibilities. 10](#_Toc349042646)

[1.2.03 Execution Responsibilities. 10](#_Toc349042647)

[2. Program Protection Summary. 10](#_Toc349042648)

[2.1. Schedule. 10](#_Toc349042649)

[2.2. CPI and Critical Functions and Components Protection. 11](#_Toc349042650)

[2.2.01 CPI and Critical Countermeasures Summary. 11](#_Toc349042651)

[3. Critical Program Information (CPI) and Critical Components. 12](#_Toc349042652)

[3.1. Identification Methodology. 12](#_Toc349042653)

[3.1.01 CPI Identification and Criticality Analysis Participants. 13](#_Toc349042654)

[3.1.02 Timing of Identification and Updates to CPI and Mission Critical Functions and Components. 13](#_Toc349042655)

[3.1.03 Process for Identifying CPI, including Inherited CPI. 13](#_Toc349042656)

[3.1.04 Approach for Performing Criticality Analysis. 13](#_Toc349042657)

[3.2. Inherited CPI and Critical Components. 13](#_Toc349042658)

[3.2.01 Inherited Items Approach. 13](#_Toc349042659)

[3.2.02 Inherited CPI and Critical Components Table. 14](#_Toc349042660)

[3.3. Organic CPI and Critical Components. 14](#_Toc349042661)

[4. Horizontal Protection. 15](#_Toc349042662)

[4.01 Identify the person or office responsible for horizontal protection. 15](#_Toc349042663)

[4.02 Horizontal Protection Information. 15](#_Toc349042664)

[4.03 Alignment and Issue Resolution of Protection of Horizontal CPI. 15](#_Toc349042665)

[4.04 Specify when the Program will Create/Update its Acquisition Security Database (ASDB) Record. 15](#_Toc349042666)

[5. Threats, Vulnerabilities, and Countermeasures. 16](#_Toc349042667)

[5.01 Summary of CPI Threats, Vulnerabilities, and Countermeasures. 16](#_Toc349042668)

[5.1. Threats. 17](#_Toc349042669)

[5.1.01 Threat Products POC and Timing. 17](#_Toc349042670)

[5.1.02 Threat Products Description. 17](#_Toc349042671)

[5.1.03 Threat Products Update Frequency. 17](#_Toc349042672)

[5.1.04 Threat Products References. 17](#_Toc349042673)

[5.1.05 Identified Threats. 18](#_Toc349042674)

[5.2. Vulnerabilities. 19](#_Toc349042675)

[5.2.01 Potential CPI and Critical Component Vulnerabilities. 19](#_Toc349042676)

[5.2.02 New Vulnerabilities Identification Process. 19](#_Toc349042677)

[5.2.03 Vulnerabilities Identification POC and Update Frequency. 19](#_Toc349042678)

[5.2.04 Specify the Frequency that the Vulnerabilities be Re-assessed. 20](#_Toc349042679)

[5.2.05 Specify the Way in which Vulnerabilities will be Identified and Mitigated. 20](#_Toc349042680)

[5.3. Countermeasures. 20](#_Toc349042681)

[5.3.01. Countermeasures Selection Approach. 20](#_Toc349042682)

[5.3.02. Countermeasures Implementation Responsibility. 20](#_Toc349042683)

[5.3.03. Protection Requirements Incorporation into Contracts. 20](#_Toc349042684)

[5.3.04. Countermeasures Implementation Descriptions. 20](#_Toc349042685)

[5.3.05. Countermeasure Implementation Plan vs Actual Tracking. 21](#_Toc349042686)

[5.3.1. Anti-Tamper (AT). 21](#_Toc349042687)

[5.3.2. Information Assurance (IA). 21](#_Toc349042688)

[5.3.3. Software Assurance. 23](#_Toc349042689)

[5.3.4. Supply Chain Risk Management. 25](#_Toc349042690)

[5.3.5. System Security Engineering. 27](#_Toc349042691)

[5.3.6. General Countermeasures. 27](#_Toc349042692)

[6. Other System Security-Related Plans and Documents. 28](#_Toc349042693)

[6.01 Other System Security-Related Plans and Documents Table. 28](#_Toc349042694)

[6.02 Key Commitments Table. 28](#_Toc349042695)

[7. Program Protection Risks. 29](#_Toc349042696)

[7.01. Program Protection Risks Integration. 29](#_Toc349042697)

[7.02 Residual Risks and Unmitigated Risks Identification. 29](#_Toc349042698)

[7.03. Risk Cube and Mitigation Plan for the top Program Protection Risks. 29](#_Toc349042699)

[8. Foreign Involvement. 29](#_Toc349042700)

[8.01. Foreign Involvement Summary. 29](#_Toc349042701)

[8.02. Applicable Technology Security and Foreign Disclosure (TS&FD) Processes. 30](#_Toc349042702)

[8.03. Previous Sales to Foreign Allies. 30](#_Toc349042703)

[8.04. Addressing of Export Requirements/Restrictions and Responsibilities. 30](#_Toc349042704)

[8.1. Defense Exportability Features. 30](#_Toc349042705)

[8.1.1. Foreign Military Sales and Direct Commercial Sales Potential Risk to Program. 30](#_Toc349042706)

[8.1.2. DEF Candidate Viability. 30](#_Toc349042707)

[8.1.3. Include a hotlink to the relevant DEF discussion. 30](#_Toc349042708)

[9. Processes for Management and Implementation of PPP. 31](#_Toc349042709)

[9.1. Audits/Inspections. 31](#_Toc349042710)

[9.2. Engineering/Technical Reviews. 31](#_Toc349042711)

[9.2.1. Addressing of System Security Requirements. 31](#_Toc349042712)

[9.2.2. Program Protection Entry/Exit Criteria. 31](#_Toc349042713)

[9.3. Verification and Validation. 31](#_Toc349042714)

[9.3.1. System security requirements testing integration. 31](#_Toc349042715)

[9.3.2. Link to relevant discussion in T&E documents. 31](#_Toc349042716)

[9.4. Sustainment. 32](#_Toc349042717)

[9.4.1. Program Protection requirements and considerations in sustainment. 32](#_Toc349042718)

[9.4.2. Link to the relevant Lifecycle Sustainment Plan (LCSP) language. 32](#_Toc349042719)

[10. Processes for Monitoring and Reporting Compromises. 32](#_Toc349042720)

[10.1. CPI Compromise/Supply Chain Exploit Response Plan/procedure. 32](#_Toc349042721)

[10.2. Anti-Tamper Event or Supply Chain exploit Definition. 32](#_Toc349042722)

[11. Program Protection Costs. 32](#_Toc349042723)

[11.1. Security Costs. 32](#_Toc349042724)

[11.1.1. Security Costs above NISPOM Requirements. 33](#_Toc349042725)

[11.1.2. SCIFs or Other Secure Facilities Construction Requirements. 33](#_Toc349042726)

[11.1.3. Limited Access Rosters or Other Similar Instruments Cost. 33](#_Toc349042727)

[11.2. Acquisition and Systems Engineering Protection Costs. 33](#_Toc349042728)

[11.2.1. Acquisition and Systems Engineering Protection Costs Table. 33](#_Toc349042729)

[11.2.2. Non-recurring Program Protection Engineering Costs Accounting. 34](#_Toc349042730)

[11.2.3. Projected Cost-benefit Tradeoffs Approach in Countermeasure Selection. 34](#_Toc349042731)

[Appendix A: Security Classification Guide. 35](#_Toc349042732)

[Appendix B: Counterintelligence Support Plan. 36](#_Toc349042733)

[Appendix C: Criticality Analysis. 37](#_Toc349042734)

[Appendix D: Anti-Tamper Plan. 39](#_Toc349042735)

[Appendix D-1: Anti-Tamper Plan Waiver. 39](#_Toc349042736)

[Appendix E: Acquisition Information Assurance (IA) Strategy. 40](#_Toc349042737)

Introduction – Purpose and Update Plan.

### 1.0.1 Users of PPP.

Click here to enter text.

Guidance: Who will use the PPP?

### 1.0.2 Alignment with Contractor’s Program Protection Implementation Plan(s) (PPIP).

Click here to enter text.

Guidance: What is the plan to align Prime Contractor Program Protection Implementation Plan(s) (PPIP) with this PPP if they are written?

### 1.0.3 Contractor’s Responsibility for Program Protection.

Click here to enter text.

Guidance: What aspects of Program Protection will you ask the contractor to do?

### 1.0.4 Timing of and Criteria for PPP updates.

Click here to enter text.

Guidance: Summarize the timing of PPP updates (e.g. prior to milestone, prior to export decision, following Systems Engineering Technical Review).

### 1.0.5 Update Authority.

Click here to enter text.

Guidance: Describe the update authority.

### 1.0.6 Approval Authority for Different Updates.

Click here to enter text.

Guidance: Describe the update authority for different updates.

### 1.0.7 PPP Update Record.

Click here to enter text.

Guidance: Provide a table listing PPP updates

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 1.0-1 PPP Update Record (mandated)** | | | |
| **Revision Number** | **Date** | **Changes** | **Approved By** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Technology/System Description.

### Link to Reference Document.

Click here to enter text.

Guidance: Reference and include a link/direction to the appropriate acquisition document (e.g.; Technology Development Strategy, Acquisition Strategy) that describes the technology/system.

### Program Information.

Click here to enter text.

Guidance: Reference and include a link/direction to the appropriate acquisition document (e.g.; Technology Development Strategy, Acquisition Strategy) that describes the technology/system and the project/program for which it will be developed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 1.1-1 Program Information** | | | |
| **Program Name** | **ACAT Level** | **Mission Assurance Category (MAC)** | **Last Milestone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Program Protection Responsibilities.

Click here to enter text.

*Guidance: Who is responsible for Program Protection on the program? The chain of responsibility for all aspects of Program Protection should be clear. Include contact information for Program Protection leads/resources/SMEs. What aspects are each of these resources responsible for? For every countermeasure being implemented, identify who is responsible for execution. Include relevant PEO/SYSCOM contacts as well.*

### 1.2.01 Countermeasure Execution Responsibility.

Click here to enter text.

*Guidance: Who is responsible for Program Protection on the program? The chain of responsibility for all aspects of Program Protection should be clear*

### 1.2.02 Program Protection Responsibilities.

Click here to enter text.

*Guidance: Include contact information for Program Protection leads/resources/SMEs. What aspects are each of these resources responsible for?*

### 1.2.03 Execution Responsibilities.

Click here to enter text.

Guidance: Identify who is responsible for execution for every countermeasure being implemented. Include relevant PEO/SYSCOM contacts as well.

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 1.2-1 Program Protection Responsibilities (mandated) (sample)** | | | |
| **Title/Role** | **Name** | **Location** | **Contact Info** |
| Program Manager |  |  |  |
| Lead Systems Engineer |  |  |  |
| Program Protection Lead |  |  |  |
| Anti-Tamper Lead |  |  |  |
| Info. Assurance Lead |  |  |  |
| Software Assurance Lead |  |  |  |
| SCRM Lead |  |  |  |
|  |  |  |  |

Program Protection Summary.

## Schedule.

Click here to enter text.

Guidance: A Program Protection schedule overlaid on to the program's master schedule (milestones, systems engineering technical reviews, etc.) includes the following:

* CPI and critical function/component identification/updates
* Acquisition Security Database (ASDB) updates
* Threat assessment requests
* Vulnerability assessments, red teams, etc.
* Security Audits/Inspections
* Engagement with Systems Engineering Technical Reviews (e.g. subsystem
* Preliminary Design Reviews for critical components)
* Countermeasure (e.g. Anti-Tamper, Information Assurance) testing/verification
* events
* Foreign involvement events (Exportability likelihood assessment, Cooperative Development, License Requests, etc.)

**Program Protection activities and events should be integrated in overall program scheduling.**

## CPI and Critical Functions and Components Protection.

Click here to enter text.

Guidance: List all CPI and critical functions and components over the lifetime of the program (including inherited and organic) mapped to the security disciplines of the countermeasures being applied in Table 2.2-1 of the Program Protection Plan Outline and Guidance (Version 1.0, July 2011). For each countermeasure being implemented, list the responsible party for execution in Section 2.1 (above).

### 2.2.01 CPI and Critical Countermeasures Summary.

Click here to enter text.

Guidance: Table 2.2-1 is meant to summarize the protection scheme/plan for the program. The detail supporting this summary assessment (including the threats and vulnerabilities to which the selected countermeasures apply) is planned for and documented in the subsequent sections of the document.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table 2.2-1 CPI and Critical Components Countermeasure Summary (mandated) (sample)** | | | | | | | | | | | | | | | | | | |
|  | **#** | **Protected Item (Inherited and Organic)** | **Countermeasures** | | | | | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| **CPI** | 1 | Algorithm QP | X | X | X | X | X | X | X | X | X | X |  |  |  | X | X |  |
| 2 | System Security Configuration |  |  |  |  |  |  |  |  |  |  | X |  |  | I |  |  |
| 3 | Encryption Hardware | X | X | X | X | X | X | X | X |  |  |  | X |  | X |  |  |
| 4 | IDS Policy Configuration | X | X | X | X | X | X | X | X |  |  |  |  |  | X |  |  |
| 5 | IDS Collected Data | X | X | X | X | X | X | I |  |  |  |  |  |  |  | I |  |
| 6 | KGV-136B | X | X | X | X |  |  | I | X | I |  |  |  | I |  |  |  |
| **Critical Components** | 7 | iDirect M1D1T Hub-Line Card | X | X | X | X | X | X | X | X |  |  |  | X | X | X |  |  |
| 8 | Cisco Router IOS with Advance Security Option (ASO) | X | X | X | X | X | X |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | **KEY [Examples Included: UPDATE THIS LIST ACCORDING TO PROGRAM]** | | | | | | | | | | | | | | | |  |
|  |  |  | **General CMs** | | | | **Research and Technology Protection CMS** | | | | | **Trusted Systems Design CMs** | | | | | |  |
|  | **Key** | |  |  |  |  |  |  |  |
|  | X = Implemented | | 1 Personnel Security | | | | 8 Transportation Mgmt | | | | | 11 IA/Network Security | | | | | |  |
|  | I = Denotes protection already implemented if CPI is inherited | | 2 Physical Security | | | | 9 Anti-Tamper | | | | | 12 Communication Security | | | | | |  |
|  | 3 Operations Security | | | | 10 Dial-down Functionality | | | | | 13 Software Assurance | | | | | |  |
|  | 4 Industrial Security | | | |  |  |  |  |  | 14 Supply Chain Risk Management | | | | | |  |
|  | 5 Training | | | |  |  |  |  |  | 15 System Security Engineering (SSE) | | | | | |  |
|  |  |  | 6 Information Security | | | |  |  |  |  |  | 16 Other | | | | | |  |
|  |  |  | 7 Foreign Disclosure/ Agreement | | | |  |  |  |  |  |  |  |  |  |  |  |  |

Critical Program Information (CPI) and Critical Components.

Identification Methodology.

Guidance: The end-to-end system must be considered, including items such as mission packages, government furnished components, and interdependent systems that may be outside a program manager's control.

* CPI and mission critical functions and components must be identified by a multi-disciplined group.
* Criticality analysis should be led by systems engineers and mission/operator representatives.
* CPI identification should be led by technology protection and security specialists.
* Information regarding these components and/or technologies must be considered for protection.
* Criticality analysis updates should be tied to Systems Engineering Technical Reviews.
* Inherited CPI is CPI from other acquisition programs, subsystems, or projects that are being incorporated or implemented into this program.
* Early in the program this section will reflect intentions. Updates to this section will provide a record of work completed and any remaining.

3.1.01 CPI Identification and Criticality Analysis Participants.

Click here to enter text.

Guidance: Describe the methodology that will be used to identify CPI and mission critical functions and components in accordance with DoDI 5200.391 and DoDI 5000.022 including the CPI identification and criticality analysis participants.

### 3.1.02 Timing of Identification and Updates to CPI and Mission Critical Functions and Components.

Click here to enter text.

Guidance: Describe the methodology that will be used for the timing of identification and updates to CPI and mission critical functions and components.

### 3.1.03 Process for Identifying CPI, including Inherited CPI.

Click here to enter text.

Guidance: Describe the process for identifying CPI, including inherited CPI.

### 3.1.04 Approach for Performing Criticality Analysis.

Click here to enter text.

Guidance: Describe the approach for performing criticality analysis.

Inherited CPI and Critical Components.

### 3.2.01 Inherited Items Approach.

Click here to enter text.

Guidance: Summarize the approach to identifying and managing Program Protection risks for any inherited CPI or critical components. Identify the system from which the inherited item comes. Specify whether the system will be protected in the same manner in which it was originally protected. Indicate variances in usage and plans for the adjustment of countermeasures as appropriate.

### 3.2.02 Inherited CPI and Critical Components Table.

Click here to enter text.

Guidance: Summarize the approach to identifying and managing Program Protection risks for any inherited CPI or critical components. Identify the POC for questions regarding the inherited system(s). Specify the way in which the program will interact with the inherited system(s) to ensure horizontal protection.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Table 3.2-1 Inherited CPI and Critical Components (mandated)** | | | | | | |
|  | **Inherited Critical Item** | **Parent Program** | **Original Use** | **Planned Use** | **Variation in CMs?** | **Inherited Program POC** |
| **CPI** |  |  |  |  |  |  |
| **Critical Components** |  |  |  |  |  |  |

## Organic CPI and Critical Components.

Click here to enter text.

Guidance: As CPI and Critical Components are identified, track them in Table 3.3-1 below.

* Identify CPI and critical components, and summarize the effects or consequences if they are compromised. Track any adds/changes/deletions from this list over the course of the program with rationale for the edit.
* Where will the CPI and critical components be physically located during the acquisition lifecycle? Indicate whether or not contractor PPIPs are in place to flow protection requirements to contractor locations.
* Show traceability from mission-level documents (JCIDS Key Performance Parameters, Key System Attributes, etc.) and Critical Technology Elements (CTE) to the system architecture.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table 3.3-1: Organic CPI and Critical Components (mandated)** | | | | | | | | |
|  | Assessment Date(s): 22 December 2009 | | | | | | | |
|  | **CPI/CC** | **Consequence of Compromise** | **Status/Date & Justification for Status Change** | | **Traceable CTEs, KPPs, etc.** | **Export Control Areas** | **Physical Location** | **System Location PPIP Exists?** |
| **CPI** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Critical Components** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Horizontal Protection.

## 4.01 Identify the person or office responsible for horizontal protection.

Click here to enter text.

Guidance: Identify the person or office responsible for horizontal protection.

## 4.02 Horizontal Protection Information.

Click here to enter text.

Guidance: Identify other programs or weapons systems with CPI similar to this program.

## 4.03 Alignment and Issue Resolution of Protection of Horizontal CPI.

Click here to enter text.

Guidance: Specify the way in which the program will align protection of horizontal CPI. Include the way in which issues/disagreements about protection of horizontal CPI will be resolved.

## 4.04 Specify when the Program will Create/Update its Acquisition Security Database (ASDB) Record.

Click here to enter text.

Guidance: Specify when the program will create/update its Acquisition Security Database (ASDB) record.

The ASDB and associated registration/help information is located on SIPRNET at <https://asdb.strikenet.navy.smil.mil> . The program ASDB record should be created as soon as CPI is identified and updated periodically, as changes occur and at each subsequent milestone. Critical Functions/Components are not identified in the ASDB. Upon creation of an ASDB record, programs should use the search capabilities to identify other programs with potentially similar CPI and follow up with their POCs to ensure horizontal protection.

See Table 4.0-1 Horizontal Protection Information.

|  |  |  |
| --- | --- | --- |
| **Table 4.0-1: Horizontal Protection Information (mandated)** | | |
| **Date of Last ASDB Update: Date of Next ASDB Update:** | | |
| **CPI** | **Other Programs With Same of Similar CPI** | **Pending Adjudications of CPI? (Y/N)** |
|  |  |  |
|  |  |  |
|  |  |  |

Threats, Vulnerabilities, and Countermeasures.

## 5.01 Summary of CPI Threats, Vulnerabilities, and Countermeasures.

Click here to enter text.

Guidance:

* Summarize any identified threats and vulnerabilities to CPI and critical functions/components in Table 5.0-1 below. Also identify any countermeasures selected to mitigate risks of compromise.
* This table should be updated over time as the information is identified; early in the program, identify the plan for obtaining this information in Sections 5.1-5.3 below.
* The numbers in the threat and vulnerabilities tables should correspond to the numbered rows in the threat table (5.1-2) and vulnerability table (5.2-1) below. All CPI and critical functions/components should be reflected in the table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Table 5.0-1 Summary of CPI Threat, Vulnerabilities, and Countermeasures (mandated) (sample)** | | | | |
|  | **CPI/CC (and CC supplier) Section 2.0** | **Threats Section 5.1** | **Vulnerabilities Section 5.2** | **Countermeasures Section 5.3** |
| **CPI** | **Algorithm** | **4, 5, 7, 13-15** | **1, 2** | **Anti-Tamper, SSE, Supply Chain Risk Management** |
| **System/Security Configuration** | **1, 9, 14, 15** | **1** | **Secure storage of configuration; Supplier Assurance** |
| **Encryption Hardware** | **2, 9, 14** | **2** | **Supply Chain Risk Management, NSA encryption device** |
| **Critical Components** | **iDirect M1D1T Hub-line Card** | **2, 8, 9, 14** | **3** | **Communication Security; Sofgtware Assurance; SCRM** |
| **Cisco Router IOS with ASO** | **2, 6, 8, 9, 14** | **4** | **Supply Chain Risk Management** |

Threats.

### 5.1.01 Threat Products POC and Timing.

Click here to enter text.

Guidance: Identify the person or office responsible for requesting and receiving threat products. Specify when those threat products will be requested. Identify the person or office in the intelligence community responsible for supporting these requests. Include these contacts in the table in Section 1.2.

### 5.1.02 Threat Products Description.

Click here to enter text.

Guidance: Identify the threat products to be requested for the program, including when and how they will they be used.

### 5.1.03 Threat Products Update Frequency.

Click here to enter text.

Guidance: Specify the frequency of which the threat products will be updated.

### 5.1.04 Threat Products References.

Click here to enter text.

Guidance: List any threats identified for threat products already received.

As threat products are received, reference these documents in Table 5.1-1. This table should be comprehensive by Milestone B. For the Supply Chain Threat Assessments, document each critical component supplier (or potential supplier) that has been assessed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Table 5.1-1 Threat Product References (mandated) (sample)** | | | | |
| **Title of Program-Specific or Other Threat Products Used for PPP Threat Analysis** | **Classification** | **Document Date** | **Organization(s) Producing the Product** | **Reference/Link to Product** |
| **Formal Threat Reports** | | | | |
| **AFOSI Counterintelligence Assessment/Report** | **S** | **Jul-02** | **HQ Office of Special Investigations** |  |
| **AFOSI Department of Defense Threat Assessment** | **S** | **Dec-07** | **Office of Special Investigations** |  |
| **Capstone Threat Assessment (CTA)** | **U-S** | **Dec-02** | **Defense Intelligence Agency** |  |
| **Foreign Technology Assessment** | **U** | **Feb-04** | **Counterintelligence Service** |  |
| **Integrated Threat Assessment (ITA)** | **U-S** | **Jan-02** | **Service for Special Assess Programs** |  |
| **Technology Targeting Risk Assessment (TTRA)** | **U-S** | **Mar-06** | **Defense Intelligence Agency** |  |
| **System Threat Assessment Report (STAR)** | **S** | **Jan-07** | **Defense Intelligence Agency** |  |
| **Supply Chain Threat Assessments** | | | | |
| **iDirect M1D1T Hub-line Card Assessment** | **TS/SCI** | **Apr-09** | **Defense Security Service** |  |
| **Cisco Router IOS with ASO** | **TS/SCI** | **Apr-09** | **Defense Security Service** |  |
| **Other Threat Documents** | | | | |
| **Technology Collection Trends in the U.S. Defense Industry** | **U** | **Oct-06** | **Defense Security Service** |  |
| **Targeting U.S. Technologies** | **U** | **Feb-06** | **Defense Security Service** |  |

### 5.1.05 Identified Threats.

Click here to enter text.

Guidance: Summarize the threats identified in Table 5.1-2 of the Program Protection Plan Outline and Guidance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 5.1-2 Identified Threats (mandated) (sample)** | | | |
| **T#** | **Threat** | **Description** | **Consequence of threat realization** |
| 1 | HUMINT Collection | Country X is actively targeting CPI #3 at Location B | Compromise of U.S. technology lead |
| 2 | Malicious Code Insertion | Country Y is known to have inserted malware into the software that Critical Component #2 depends on | Degraded or untrustworthy performance of targeting module |
| 3 |  |  |  |
| 4 |  |  |  |
|  |  |  |  |

Vulnerabilities.

### 5.2.01 Potential CPI and Critical Component Vulnerabilities.

Click here to enter text.

Guidance: Specify the vulnerabilities identified to date.

Summarize the results of any vulnerability assessments, red teams, etc. performed to date in Table 5.2-1 below.

|  |  |  |
| --- | --- | --- |
| **Table 5.2-1 Potential CPI and Critical Component Vulnerabilities (mandated)** | | |
| **V#** | **CPI/Critical Components** | **Identified Vulnerabilities** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

### 5.2.02 New Vulnerabilities Identification Process.

Click here to enter text.

Guidance: How will the program identify new vulnerabilities (both system-level and in the development environment) to the CPI and mission-critical functions and components?

### 5.2.03 Vulnerabilities Identification POC and Update Frequency.

Click here to enter text.

Guidance: Identify the person or office responsible for identifying vulnerabilities to the CPI and mission-critical functions and components, as well as the frequency for updates. The person or office should be included in the table in Section 1.2.

### 5.2.04 Specify the Frequency that the Vulnerabilities be Re-assessed.

Click here to enter text.

Guidance: Specify the frequency that the vulnerabilities be re-assessed.

### 5.2.05 Specify the Way in which Vulnerabilities will be Identified and Mitigated.

Click here to enter text.

Guidance: Specify the way in which vulnerabilities will be identified and mitigated.

Countermeasures.

### 5.3.01. Countermeasures Selection Approach.

Click here to enter text.

Guidance: How will countermeasures be selected to protect CPI and critical functions/components?

### 5.3.02. Countermeasures Implementation Responsibility.

Click here to enter text.

Guidance: Who has the responsibility for their implementation? Include in the table in Section 1.2.

### 5.3.03. Protection Requirements Incorporation into Contracts.

Click here to enter text.

Guidance: How will contracts supporting the acquisition program incorporate protection requirements? Indicate the RFP Contract Line Item Number (CLIN) or Data Item Description (DID) that will be used to ensure that CPI and critical functions/components are protected in the development environment and on the system.

### 5.3.04. Countermeasures Implementation Descriptions.

Click here to enter text.

Guidance: Succinctly describe the implementation of each countermeasure used to protect CPI and critical functions and components. Be specific: If SCRM Key Practices apply, describe which ones; if using Software Assurance techniques, explain which ones.

### 5.3.05. Countermeasure Implementation Plan vs Actual Tracking.

Click here to enter text.

Guidance: Indicate planned implementation and actual implementation as the PPP evolves. Explain deviations from the plan. At a minimum, address implementation of the countermeasures in Section 5.3.1- 5.3.5 or rationale for not using them.

Anti-Tamper (AT).

#### 5.3.1.01. AT Requirements Identification and Plan Development Responsibilities.

Click here to enter text.

Guidance: Who will identify AT requirements and who is responsible for developing an AT plan?

#### 5.3.1.02. AT Plan Development Schedule.

Click here to enter text.

Guidance: When will the AT Plan be completed? Include plans for engaging with the Component AT lead and Executive Agent for AT. If an AT Plan or AT Plan Waiver has been developed, submit as an Appendix.

Information Assurance (IA).

Guidance: IA countermeasures planning should account for the system being acquired and any support information systems that may contain or host CPI and critical functions and components. The Acquisition IA Strategy documents the plan for implementing IA specifically on the system being acquired. IA controls can also be applied to protect CPI and critical functions and components as they are handled/transmitted across contractor or partner systems. For example, contractor development environments may host CPI and should be evaluated for protection.

#### 5.3.2.01. IA Countermeasures Adequacy Assessment Responsibility.

Click here to enter text.

Guidance: Who is responsible for assessing the adequacy of IA countermeasures for CPI?

#### 5.3.2.02. IA Schedule.

Click here to enter text.

Guidance: What are the key IA schedule milestones?

#### 5.3.2.03. Implementation of IA Protections for DoD Systems Hosting CPI.

Click here to enter text.

Guidance: How will the appropriate implementation of IA protections for DoD information systems hosting CPI be ensured?

#### 5.3.2.04. Implementation of IA Protections for non- DoD Systems Hosting CPI.

Click here to enter text.

Guidance: How will the appropriate implementation of IA protections for contractor-owned non-DoD information systems hosting CPI be ensured?

##### 5.3.2.04.01. IA Controls Negotiations.

Click here to enter text.

Guidance: How will IA controls be negotiated with contractors?

##### 5.3.2.04.02. Responsibility for IA Controls Flow to Subcontractors.

Click here to enter text.

Guidance: Who will ensure these controls are flowed down to subcontractors?

##### 5.3.2.04.03. Responsibility for Inventory of CPI Hosted on Contractor Systems.

Click here to enter text.

Guidance: Who will keep an inventory of CPI hosted on contractor information systems?

#### 5.3.2.05. Implementation of IA Protections for Acquired System Hosting CPI.

Click here to enter text.

Guidance:

How will the appropriate implementation of IA protections for the system being acquired (if it includes on-board CPI) be ensured?

Include the Component CIO approved Acquisition IA Strategy as an Appendix. (See Appendix E description in this document)

Software Assurance.

#### 5.3.3.01. Software Assurance Responsibility.

Click here to enter text.

Guidance: Who is responsible for Software Assurance?

#### 5.3.3.02. Software Design and Testing Approach.

Click here to enter text.

Guidance: How will software be designed and tested to assure protection of critical functionality and CPI?

#### 5.3.3.03. Application of Software Assurance Countermeasures.

Click here to enter text.

Guidance: How will software architectures, environments, designs, and code be evaluated with respect to CVE (Common Vulnerabilities and Exposures), CAPEC (Common Attack Pattern Enumeration and Classification), and CWE (Common Weakness Enumeration)?

* CVE - Used to identify and coordinate SW vulnerabilities that enable various types of attacks.
* CAPEC - Used for the analysis of common destructive attack patterns
* CWE - Used to examine software architecture/design and source code for weaknesses.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table 5.3.3-1 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 |
| **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 | | | | | | | |

#### 5.3.3.04. COTS Software and Software of Unknown Pedigree Protection, Testing/vetting.

Click here to enter text.

Guidance: How will COTS software and software of unknown pedigree (i.e., software from sources buried in the supply chain) be protected and tested/vetted?

#### 5.3.3.05. How will the Development Environment be Protected?

Click here to enter text.

Guidance: How will the critical functions and CPI be protected in the operational system?

##### 5.3.3.05.01. List the Development Environment Tools

Click here to enter text.

Guidance: List the development environment tools.

#### 5.3.3.06. Development Environment Access.

Click here to enter text.

Guidance: How will the development environment be protected? Who has access to the development environment?

##### 5.3.3.06.01. Development Environment Access List Management.

Click here to enter text.

Guidance: Who will be responsible for maintaining a list of cleared, US citizens as well as foreign nations/nationals that have access?

##### 5.3.3.06.02. Where will the list be stored, and how often will it be updated?

Click here to enter text.

Guidance: Where will the list be stored, and how often will it be updated?

#### 5.3.3.07. Planned vs. Actual Testing/Evaluation Rates Deviation.

Click here to enter text.

Guidance: P/A indicates planned/actual – explain any deviations from planned testing/evaluation rates. For further details see key practices 9,11,16,17,19,21 and 23 in the "Key Practices and Implementation Guide for DOD Comprehensive National Cyber Initiative 11 Supply Chain Risk Management Pilot Program.”

### Supply Chain Risk Management.

#### 5.3.4.01. Supply Chain Risk Management.

Click here to enter text.

Guidance: How will the program manage supply chain risks to CPI and critical functions and components?

#### 5.3.4.02. Supply Chain Threat Assessments Use and Influence.

Click here to enter text.

Guidance: Explain how supply chain threat assessments will be used to influence system design, development environment, and procurement practices.

#### 5.3.4.03. Supply Chain Threat Assessments Use and Influence Responsibiity.

Click here to enter text.

Guidance: Who has this responsibility?

#### 5.3.4.04. Supply Chain Threat Assessments Request Timing.

Click here to enter text.

Guidance: When will threat assessments be requested?

#### Trusted Suppliers.

Click here to enter text.

Guidance:

* Will any ASICs require trusted fabrication?
* How will the program make use of accredited trusted suppliers of integrated circuit-related services?

##### 5.3.4.1.01. Trusted Fabrication of ASICs.

Click here to enter text.

Guidance: Will any ASICs require trusted fabrication?

##### 5.3.4.1.02. Utilization of Accredited Trusted Suppliers.

Click here to enter text.

Guidance: How will the program make use of accredited trusted suppliers of integrated circuit-related services?

#### 5.3.4.2 Counterfeit Prevention.

Click here to enter text.

Guidance: What counterfeit prevention measures will be in place? How will the program mitigate the risk of counterfeit insertion during Operations and Maintenance?

System Security Engineering.

#### 5.3.5.01. System Security Engineering Responsibility.

Click here to enter text.

Guidance: Identify the person or office responsible for system security engineering.

#### 5.3.5.02. System Security Engineering and System Engineering Plan.

Click here to enter text.

Guidance: Describe the linkage between system security engineering and the Systems Engineering Plan. Describe the way in which system security design considerations should be addressed.

General Countermeasures.

#### 5.3.6.01. Generic Program Countermeasures/Security Activities.

Click here to enter text.

Guidance: Summarize generic countermeasures or security activities in place that will/do apply to all program information/facilities/personnel and contribute to the protection of CPI and critical functions and components.

|  |  |
| --- | --- |
| **Table 5.3.6-1 Generic Program Countermeasure/Security Activities (mandated) (sample)** | |
| **Type Type** | **Detail** |
| COMSEC (Development Environment) | * Program Office Policy XX-XXX details program COMSEC countermeasures that are implemented at each government facility. |
| OPSEC | * Program Management Directive XX-XXX, will be tailored to satisfy specific security requirements of individual PROGRAM XYZ activities. * The PROGRAM XYZ effort will comply fully with AFI 10-701, Operations Security * The 669 AESS OPSEC Plan identifies all PROGRAM XYZ critical information. |
| Foreign Visit Program | * Program office personnel, other government organizations and contractors will adhere to approved visit procedures for the facility being visited. |
| CPI Protection Training | * The PM has instituted a tiered training program. Tier 1 is for general training of what CPI is and Tier II is for personnel who actually handle, store, develop and/or maintain CPI. All industry partners who have this PPP, implemented via DD Form 254, DoD Contract Security Classification Specifications, will implement this tier training. |
| Information Assurance (Development Environment) | * Prime Contractor network security architecture and configuration will be managed by the CIO. Network security procedures and countermeasures applicable to subnets containing Government CUI are available upon request. The program will comply with DTM 08-027 “Security of Unclassified DoD Information on Non-DoD Information Systems”. |
| Secure System Administration | * System configuration will be managed remotely by the DISA GNSC/TNC administrators. |
| Personnel Security | * The 669 AESS/SF is responsible for reviewing personnel security procedures at all 669 AESS and PROGRAM XYZ industry locations. This will be coordinated with DSS for industry reviews. |
| Industrial Security | * Security protection requirements will be incorporated into all PROGRAM XYZ contracting activities. Government procedures and instructions for preparing DD Forms 254, Contract Security Classification Specifications, will ensure that contractors are provided quality acquisition security, Program Protection, and classification management guidance. |

Other System Security-Related Plans and Documents.

## 6.01 Other System Security-Related Plans and Documents Table.

Click here to enter text.

Guidance: Reference relevant acquisition or system security-related documents.

|  |  |  |
| --- | --- | --- |
| **Table 6.0-1: Other System Security-Related Plans and Documents (mandated) (sample)** | | |
| **Plan** | **Organization** | **Link/POC** |
| Counterintelligence Support Plan (CISP) | Service CI |  |
| Test & Evaluation Master Plan | TEMP Approval Authority |  |
| Systems Engineering Plan | SEP Approval Authority |  |
| Software Secure Coding Standards | Contractor SW Design Lead |  |
| Trusted Software Design Techniques | Contractor SW Design Lead |  |
| Secure Software Process Standards | Contractor SW Design Lead |  |
| Foreign Travel Training | Contractor FSO |  |
| Foreign Visit Processes | Contractor FSO |  |

## 6.02 Key Commitments Table.

Click here to enter text.

Guidance: If Technical Assistance Agreements, Memoranda of Agreement (MOA), Memoranda of Understanding (MOU), or other similar agreements have been signed, reference or link to them in an additional table with a description of the key commitments.

Program Protection Risks.

## 7.01. Program Protection Risks Integration.

Click here to enter text.

Guidance: Describe the way in which Program Protection risks (cost, schedule, technical) will be integrated with overall Program risk management.

## 7.02 Residual Risks and Unmitigated Risks Identification.

Click here to enter text.

Guidance: Discuss the approach to identifying residual risks of CPI and critical function and component compromise after countermeasure implementation. Identify any unmitigated risks.

## 7.03. Risk Cube and Mitigation Plan for the top Program Protection Risks.

Click here to enter text.

Guidance: Include a risk cube and mitigation plan for the top Program Protection risks.

Foreign Involvement.

## 8.01. Foreign Involvement Summary.

Click here to enter text.

Guidance: Summarize any international activities and any plans for, or known, foreign cooperative development or sales of the system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Table 8.0-1 Foreign Involvement Summary (mandated) (sample)** | | | | |
| **This system is US ONLY (Yes, No, Unknown): Yes** | | | | |
| **This system is intended for CONUS deployment only (Yes, No, Unknown): No. It is intended for global deployment.** | | | | |
| **Approved Disclosures of CPI: TBD** | | | | |
| **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?** |
| **IC** | **M** | **Perceived** | **None** | **Pangaea** |

## 8.02. Applicable Technology Security and Foreign Disclosure (TS&FD) Processes.

Click here to enter text.

Guidance: 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?

## 8.03. Previous Sales to Foreign Allies.

Click here to enter text.

Guidance: Have previous generations of this system been sold to foreign allies? Have similar systems been sold?

## 8.04. Addressing of Export Requirements/Restrictions and Responsibilities.

Click here to enter text.

Guidance: How will export requirements/restrictions be addressed if a foreign customer/sale is identified? Who is responsible for implementing these requirements?

Defense Exportability Features.

### 8.1.1. Foreign Military Sales and Direct Commercial Sales Potential Risk to Program.

Click here to enter text.

Guidance: What are the impacts and risks to the program from foreign military sales and direct commercial sales? Who is responsible for managing these?

### 8.1.2. DEF Candidate Viability.

Click here to enter text.

Guidance: Will the program be a viable DEF candidate to develop, plan, and design an export variant during the research and development phase?

### 8.1.3. Include a hotlink to the relevant DEF discussion.

Click here to enter text.

Guidance: Include a hotlink to the relevant DEF discussion in the Technology Development Strategy and/or Acquisition Strategy.

Processes for Management and Implementation of PPP.

Guidance: There are several types of checking PPP implementation. Audits/inspections are used to ensure compliance with applicable laws, regulations, and policies. Engineering reviews are used to ensure that system security requirements are identified, traceable and met throughout the acquisition lifecycle.

## Audits/Inspections.

Click here to enter text.

Guidance: Summarize the timing of security audits/inspections. Describe the way in which contractor security requirements will be enforced. Identify the person or office responsible for contractor security requirements.

Engineering/Technical Reviews.

### 9.2.1. Addressing of System Security Requirements.

Click here to enter text.

Guidance: How will system security requirements be addressed in Systems Engineering Technical Reviews, functional/physical configuration audits, etc? Who is responsible for this?

### 9.2.2. Program Protection Entry/Exit Criteria.

Click here to enter text.

Guidance: What Program Protection entry/exit criteria will be used for these reviews?

Verification and Validation.

### System security requirements testing integration.

Click here to enter text.

Guidance: Explain how the program will integrate system security requirements testing into the overall test and evaluation strategy. Who is responsible for this?

### Link to relevant discussion in T&E documents.

Click here to enter text.

Guidance: Link to relevant discussion in T&E documents.

Sustainment.

### Program Protection requirements and considerations in sustainment.

Click here to enter text.

Guidance: How will Program Protection requirements and considerations be managed in sustainment? Who is responsible for this?

### Link to the relevant Lifecycle Sustainment Plan (LCSP) language.

Click here to enter text.

Guidance: Link to the relevant Lifecycle Sustainment Plan (LCSP) language.

Processes for Monitoring and Reporting Compromises.

## CPI Compromise/Supply Chain Exploit Response Plan/procedure.

Click here to enter text.

Guidance: Summarize the plan/procedure for responding to a CPI compromise or a supply chain exploit.

## Anti-Tamper Event or Supply Chain exploit Definition.

Click here to enter text.

Guidance: What constitutes a compromise or exploit? Who is notified if one occurs? Define what constitutes an Anti-Tamper event or a Supply Chain exploit.

# Program Protection Costs.

Click here to enter text.

Guidance: Indicate where Program Protection costs are to be accounted for in the SCP and program budget. Who has the responsibility to ensure Program Protection costs are estimated and included in the programs budget and contracts?

Security Costs.

### Security Costs above NISPOM Requirements.

Click here to enter text.

Guidance: Indicate/Estimate the security costs associated with Program Protection that exceed normal NISPOM costs.

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 11.1-1 Security Costs above NISPOM Requirements (mandated)** | | | |
| **Cost Type** | **Activity** | **Responsibility** | **Cost** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Cost** |  |  | **$$** |

### SCIFs or Other Secure Facilities Construction Requirements.

Click here to enter text.

Guidance: Will SCIFs or other secure facilities require construction specifically for CPI protection?

### Limited Access Rosters or Other Similar Instruments Cost.

Click here to enter text.

Guidance: If limited access rosters or other similar instruments will be used, how much will development and maintenance of the roster cost?

Acquisition and Systems Engineering Protection Costs.

### Acquisition and Systems Engineering Protection Costs Table.

Click here to enter text.

Guidance: Indicate/estimate the design, engineering, development, testing, and other costs related to Program Protection activities (e.g. CPI identification, criticality analysis, vulnerability assessment, countermeasure development, etc.).

As costs are identified, summarize in table 11.2-1.

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 11.2-1 Acquisition and Systems Engineering Protection Costs (mandated) (sample)** | | | |
| **Cost Type** | **Activity** | **Responsibility** | **Cost** |
| Engineering | Incorporate CA, protection design alternative trade studies and system security requirements into RFP scope | PM | $$ |
| CA and design alternative trade study | Prime Contractor | $$ |
| Anti-tamper | Prime Contractor | $$ |
| Trusted Foundry | Supplier | $$ |
| Supply Chain Risk Management | Evaluate supplier lists | PM, DIA, TAC | $$ |
| Verification & Validation | Software code analysis | PM, Gunter AFB | $$ |
| V&V for anti-tamper architecture | AF AT | $$ |
| Verify satisfaction of system security requirements | PM, verification team | $$ |
| Sustainment | Anti-counterfeit measures | Depot | $$ |
| **Total Cost** |  |  | **$$** |

### Non-recurring Program Protection Engineering Costs Accounting.

Click here to enter text.

Guidance: How will non-recurring engineering costs associated with Program Protection requirements be accounted for?

### Projected Cost-benefit Tradeoffs Approach in Countermeasure Selection.

Click here to enter text.

Guidance: Describe the programs approach to using projected cost-benefit tradeoffs in countermeasure selection.

# Appendix A: Security Classification Guide.

Click here to enter text.

Guidance:

The SCG may be referenced or pointed to rather than included in the document.

# Appendix B: Counterintelligence Support Plan.

Click here to enter text.

Guidance: The CISP may be referenced or pointed to rather than included in the document.

# Appendix C: Criticality Analysis.

Guidance: The CA may be referenced or pointed to rather than included in the document (see Criticality Analysis Template in ADDM).

# Appendix D: Anti-Tamper Plan.

Click here to enter text.

Guidance:

The Anti-Tamper Plan may be referenced or pointed to rather than included in the document (see Anti-Tamper Plan Template in ADDM).

# Appendix D-1: Anti-Tamper Plan Waiver.

Click here to enter text.

Guidance:

Not all programs will require an Anti-Tamper plan.

# Appendix E: Acquisition Information Assurance (IA) Strategy.

Click here to enter text.

Guidance:

1. The reuse of existing documentation in preparing the Acquisition IA Strategy document is strongly encouraged where practicable. For example, the integrated schedule in the program's approved Acquisition 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 IA Strategy document. References to draft documents are not sufficient to support approval of the Acquisition IA 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 IA Strategies are not required for Material Development Decisions (MDD)
* Acquisition IA Strategies for Milestone A - 7 pages
* Acquisition IA Strategies for Milestone B or C - 15 pages
* Acquisition IA 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 IA Strategy be included as an appendix to the Program Protection Plan. This does not affect the current review and approval process for the Acquisition IA 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 IA Strategy documents.

5. IA threats must be included in the PPP threat table.

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. Information Assurance Requirements.

A. Sources (Applicable to MS A, B, C, FRP/FDD)

1. Mission Assurance Category and Confidentiality Level

Identify the system's MAC and Confidentiality Level as specified in the applicable capabilities document, or as determined by the system User Representative on behalf of the information owner, in accordance with DoD Instruction 8500.2. If the system architecture includes multiple segments with differing MAC and CL combinations, include a table listing all segments and their associated MAC and CL designations, as well as a brief rationale for the segmentation.

2. Baseline IA Control Sets

Identify the applicable sets of Baseline IA Controls from DoD Instruction 8500.2 that will be implemented. A listing of individual controls is not required.

3. ICD/CDD/CPD specified requirements

List any specific IA requirements identified in the approved governing capability documents (e.g. Initial Capabilities Document, Capability Development Document or Capability Production Document).

4. Other requirements

List any IA requirements specified by other authority (i.e. Component mandated).

B. IA Budget (scope and adequacy) (Applicable to MS A, B, C, FRP/FDD)

Describe how IA requirements for the full life cycle of the system (including costs associated with certification and accreditation activities) are included and visible in the overall program budget. Include a statement of the adequacy of the IA budget relative to requirements.

III. System IA Approach (high level): (Applicable to MS B, C, FRP/FDD)

A. System IA technical approach

Describe, at a high level, the IA 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 IA 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 IA 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 IA capabilities (COTS or developmental contract)

B. GFE/GFM (external programs)

C. System IA capabilities as services (commercial or government)

D. Information Systems Security Engineering (ISSE) services

E. IA professional support services to the program (commercial or government, including C&A support)

Confirm that program contracts/agreements communicate the requirement for personnel performing IA roles to be trained and appropriately certified in IA in accordance with DoD Directive 8570.01.

V. System Certification and Accreditation:

A. Process (DIACAP; DCID 6/3, etc) (Applicable to MS A, B, C, FRP/FDD)

Identify the specific Certification and Accreditation (C&A) process to be employed (e.g., DoD Information Assurance Certification and Accreditation Process (DIACAP), NSA/CSS Information Systems Certification and Accreditation Process (NISCAP), DoD Intelligence Information System (DODIIS)). If the system being acquired is platform IT without a GIG interconnection, describe any Component level process imposed to allocate and validate IA 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, Certification Authority, and User Representative for each separately accreditable system being acquired by the program.

C. C&A timeline (Applicable to MS B, C, FRP/FDD)

Include a timeline graphic depicting the target initiation and completion dates for the C&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. C&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 certification and accreditation process. If the C&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 C&A process (e.g. general descriptions of the DIACAP activities from DoDI 8510.01 and the DIACAP Knowledge Service).

VI. IA Testing:

A. Testing Integration (Applicable to MS A, B, C, FRP/FDD)

Confirm that all IA testing and C&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. IA/IA enabled products) (Applicable to MS B, C, FRP/FDD)

List any planned incorporation of IA products/IA 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. IA Shortfalls: (Include as classified annex if appropriate) (Applicable to MS B, C, FRP/FDD)

A. Significant IA shortfalls

Identify any significant IA 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 IA 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 IA Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The Information Assurance Support Environment website 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 IA Strategy document. It is recommended that the system's Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.