Program Protection Plan Evaluation Criteria

VERSION 1.1

FEBRUARY 2014

Deputy Assistant Secretary of Defense for Systems Engineering

Washington, D.C.

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). 2014. *Program Protection Plan Evaluation Criteria.* Washington, D.C.: DASD(SE).

Office of Primary Responsibility:

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030
www.acq.osd.mil/se

Introduction

This document is intended to assist Department of Defense (DoD) personnel developing and reviewing Program Protection Plans (PPP) for defense acquisition programs. It describes the criteria that DoD reviewers use when evaluating PPPs. The Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) developed the criteria to promote consistent PPPs across the Department and to ensure consistent feedback to program managers and systems engineers preparing the PPPs.

PPP developers and reviewers should refer to these criteria to assess whether a proposed PPP meets the requirements of the principal DoD policy and guidance concerning PPPs: DASD(SE) *Program Protection Plan Outline and Guidance*; Department of Defense Instruction (DoDI) 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense;" and DoDI 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks." The following list of references is not exhaustive but includes sources relevant to the PPP.

This document (Version 1.1) is intended for use with DASD(SE) *Program Protection Plan Outline and Guidance*, July 2011, (Version 1.0). Future versions of these evaluation criteria will be published to align with updates to the *Program Protection Plan Outline and Guidance.*

References

Assistant Secretary of the Air Force (Acquisition) (SAF/AQ). 2010. *Anti-Tamper (AT) Guidelines, Version 2.0*. Washington, D.C.: SAF/AQ (April).

Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Unclassified Controlled Technical Information." http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm#204.7302

Department of Defense Instruction (DoDI) 4140.67. 2013. "DoD Counterfeit Prevention Policy." Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics (April 26). www.dtic.mil/whs/directives/corres/pdf/414067p.pdf

Department of Defense Instruction (DoDI) Interim 5000.02. 2013. "Operation of Defense Acquisition System." Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics (November 25). http://www.dtic.mil/whs/directives/corres/pdf/500002_interim.pdf

Department of Defense Instruction (DoDI) 5200.39. 2010. "Critical Program Information (CPI) Protection Within the Department of Defense." Washington, D.C.: Under Secretary of Defense for Intelligence (December 28). http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

Department of Defense Instruction (DoDI) 5200.44. 2012. "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks." Washington, D.C.: DoD Chief

Information Officer/Under Secretary of Defense for Acquisition, Technology, and Logistics (November 5). http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf

Department of Defense Instruction (DoDI) 8500.2. 2003. "Information Assurance (IA) Implementation." Washington, D.C.: Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (February 6). http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

Department of Defense Instruction (DoDI) 8582.01. 2012. "Security of Unclassified DoD Information on Non-DoD Information Systems." Washington, D.C.: DoD Chief Information Officer (June 6). http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). 2013. "Program Protection." Chapter 13 in *Defense Acquisition Guidebook.* Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics. https://acc.dau.mil/dag13

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). 2011. *Program Protection Plan Outline* and *Guidance, Version 1.0.* Washington, D.C.: DASD(SE) (July). http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf

National Institute for Standards and Technology (NIST). 2013. "Security and Privacy Controls for Federal Information Systems and Organizations." NIST 800-53, Revision 4 Washington, D.C.: U.S. Department of Commerce (May). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Public Law 112-239, 112th Cong. (January 2, 2013). *National Defense Authorization Act (NDAA) for Fiscal Year 2013,* Section 933

Public Law 111-383, 111th Cong. (January 7, 2011). *Ike Skelton National Defense Authorization Act (NDAA) for Fiscal Year 2011,* Section 243.

Program Protection Plan (PPP) Evaluation Criteria

The table below parses the recommended outline for the PPP to the subsection level (i.e., 1.1, 1.2, etc.). For each subsection, the PPP Requirements column describes the required information for inclusion in that section of the PPP. The Policy and Guidance References column identifies the specific portions of the references that result in the requirement. The Criteria column indicates whether the omission or inadequate information provided in that particular section would be considered a Critical (C) comment by the reviewer, resulting in non-concurrence, or a Substantive (S) comment with suggestions provided by the reviewer for additional information or a revision.

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
	Section 1	**Update Record/Description/Points of Contact (POC)**	**Outline & Guidance (O&G), Section 1**	
1-1	**1.0**	Section provides information as outlined in Sections 1.0, 1.1 and 1.2 of the Outline and Guidance.	**O&G, Section 1**	**S**
	Section 2	**Program Protection Summary**	**O&G, Section 2**	
2-1	**2.1**	Schedule in this section has identified and mapped program protection activities against the overall program schedule. Program Management Office (PMO) has included specific PPP-related events, including but not limited to: Critical Program Information (CPI) identification, Criticality Analysis, Vulnerability Assessment, Risk Assessment, Countermeasure selection updates before each Systems Engineering Technical review (SETR), PPP updates before each milestone, Defense Intelligence Agency (DIA) Threat Assessment request submittals, Defense Exportability Features (DEF)-related activities, Anti-Tamper (AT) Concept at Milestone (MS) A, Initial AT Plan before Preliminary Design Review (PDR) and Final AT Plan before Critical Design Review (CDR), and program protection–related test events.	**O&G, Section 2.1**	**S**
2-2	**2.2 Table 2.2-1**	Table includes CPI as identified by the program office, including candidate and final inherited and organic CPI. The approval memorandum is referenced or provided.	**DoDI 5200.39 Para 4.b, 4.d, Enclosure 2, Para 6.q; O&G, Section 2.2-1**	**C**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
2-3	**2.2 Table 2.2-1**	Table identifies and decomposes Critical Functions and associated Critical Components (or potential Critical Components) to the current level of design.	**DoDI 5200.44, Para 4.d, Enclosure 2, Para 8.a(4); O&G, Section 2.2-1**	**C**
2-4	**2.2 Table 2.2-1**	Table includes information to indicate that CPI, Critical Functions, and Critical Components (including inherited and organic) are mapped to the security disciplines (Countermeasures 1-16 from key). Selected Countermeasures are accurately cross-referenced to what is documented throughout the completed document. *If AT is identified as a Countermeasure, the table and PPP are appropriately marked in accordance with AT Security Classification Guide.*	**O&G, Section 2.2; DAG Chapters 2.3.12.2. and 13.3**	**S**
	Section 3	**CPI and Critical Components**	**O&G, Section 3**	
3-1	**3.1**	CPI: Methodology for CPI identification is documented, to include candidate and final inherited and organic CPI. Methodology should be repeatable, include timing of updates, and contain a list of functional participants.	**DoDI 5200.39, Para 4.b; O&G, Section 3.1**	**S**
3-2	**3.1**	Mission Criticality Analysis: Method for Criticality Analysis is documented, to include inherited (legacy) and organic Critical Functions/Components. Section includes inherited and organic Critical Functions/components, as appropriate. Methodology should be repeatable, include timing of updates to Criticality Analysis, and contain a list of functional participants. *In updated PPPs, the process may show additional details.*	**DoDI 5200.44, Para 4.d; O&G, Section 3.1**	**S**
3-3	**3.1**	Evidence is provided that Criticality Analysis has been and will be addressed as part of the SETR process.	**O&G Section 3.1, page 10**	**S**
3-4	**3.2 Table 3.2-1**	Table has been completed for programs that have identified inherited Critical Functions/ Components, and/or CPI, as appropriate. Section is consistent with Criticality Analysis, and/or Acquisition Security Database (ASDB) and Anti-Tamper (AT) Plan, as appropriate.	**O&G, Section 3.2, Table 3.2-1**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
3-5	**3.3 Table 3.3-1**	Table has been completed with organic Critical Functions/Components, and/or CPI, as appropriate. Table is consistent with Criticality Analysis, and/or ASDB and AT Plan.	**O&G, Section 3.3,Table 3.3-1**	**S**
3-6	**3.3 Table 3.3-1**	Table indicates whether CPI resides in an Export Control Area for sale to allies/foreign customers. Table is consistent with Section 8.0 and 8.1.	**DoDI 5200.39, Para 4.a and 4.d**	**S**
3-7	**3.3 Table 3.3-1 and A_c Table C-1**	Critical Functions and Components align with the level of design detail expected at the current SETR.	**DoDI 5200.44 Section 1.a; O&G, Section 3.3**	**C**
	Section 4	**Horizontal Protection**	**O&G, Section 4**	
4-1	**4**	Section describes the methodology that will be used to resolve issues/disagreements for horizontal protection of CPI.	**O&G, Section 4**	**S**
4-2	**4**	For identified horizontal CPI, section indicates how the horizontal CPI will be protected.	**DoDI 5200.39, Para 4.c, 4.d; O&G, Section 4**	**S**
4-3	**4**	Section provides evidence that approved CPI is entered into ASDB.	**DoDI 5200.39, Enclosure 2, Para 1.e; and Para 6.g; O&G, Section 4**	**S**
	Section 5	**Threats, Vulnerabilities, and Countermeasures**	**O&G, Section 5**	
5-1	**5.0 Table 5.0-1**	Table 5.0-1 includes supply chain threats and vulnerabilities to CPI and Critical Functions/Components; supply chain risks; and Countermeasures to mitigate resulting risks. Section is consistent with Section 5.3.4.	**DoDI 5200.44 Para 4.a-e; O&G, Section 5.0**	**S**
5-2	**5.0 Table 5.0-1**	Table documents Countermeasures, including Information Assurance (IA), that are selected to mitigate risks of compromise. Section is consistent with IA Strategy and 5.3.2.	**O&G, Section 5.0**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
5-3	**5.1 Table 5.1-1**	Table indicates that DIA Threat Analysis Center (TAC) Threat Assessment Requests are developed for initial or updated Level I and selected Level II Critical Components based on Criticality Analysis (including functions that Critical Functions depend upon and those functions that have unmediated access to Critical Functions). Threat Product References document each Critical Component supplier (or potential supplier) that has been assessed.	**DoDI 5200.44 Enclosure 2 Para 8.b(2); O&G, Section 5.1; DAG Chapter 13.4.1.2**	**C**
5-4	**5.1 Table 5.1-1**	Table contains the program's list of Threat Reports and DIA TAC Reports as applicable.	**DAG Chapter 8**	**S**
5-5	**5.1 Table 5.1-2**	Threats identified in threat products from Table 5.1-1 are listed in Table 5.1-2. Possible threats may include but are not limited to TAC Report results, other supply chain threats (receiving, transmission, transportation…). IA threats are listed in Table 5.1 2: Identified Threats.	**5200.44 Para 1.d and 4.d; O&G, Appendix E, Para 5**	**C**
5-6	**5.1 Table 5.1-2**	If DIA TAC Report results are not available, PMO has assumed a medium to medium-high supplier threat for Level I and selected Level II Critical Functions and Components.	**DoDI 5200.44 Para 1.d and 4.a-e; O&G Section 5.1-2**	**S**
5-7	**5.2**	The vulnerability determination process is described at a high level including: the methodology the program will use to identify new vulnerabilities for the system and development environment, frequency/timeline for identification of new vulnerabilities, and the methodology to mitigate identified vulnerabilities.	**DoDI 5200.44, Para 4.c; O&G, Section 5.2; DAG Chapter 13.5.4**	**S**
5-8	**5.2 Table 5.2-1**	For MS A, the potential design, development, supply chain and malicious insertion CPI, and Critical Function/component vulnerabilities are listed. For MS B, C, or Full-Rate Production/Full Deployment Decision, the specific design, development, supply chain, and malicious insertion CPI and Critical Function/Component vulnerabilities are listed and assessed.	**DoDI 5200.39 Para 4.d; DoDI 5200.44 Para 4.c; O&G, Section 5.2 and 5.2-1**	**C**
5-9	**5.3**	PMO has described a methodology for selecting Countermeasures to protect Critical Functions/Components and/or CPI, as appropriate.	**O&G, Section 5.3DAG Chapter 13**	**S**
5-10	**5.3**	Countermeasures described cover prevention, detection, and response.	**DoDI 5200.44 Para 4.c, 4.d; O&G, Section 5.3**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
5-11	**5.3**	Section describes the incorporation of contract requirements for Countermeasures into: the Request for Proposal Statement of Work/Objectives, the Contract Data Requirements List items, and the system requirements either in the main section or the applicable subsection of 5.3.	**DoDI 5200.44 Para 4c5; O&G, Section 5.3**	**C**
5-12	**5.3.1**	Section identifies AT POC in either POC table, Section 3.0, or 5.3.1. Section includes plan to deliver AT Plan overlaid on Program Schedule in either Section 2.0, or schedule is contained in Section 5.3.1. Section describes plan to engage with Service AT and ATEA as appropriate. Evidence is provided that the AT Plan is submitted as an appendix to the PPP.	**DoDI 5200.39 Para 4.b; DAG Chapter 13**	**C**
5-13	**5.3.2**	POC is identified for assessing the adequacy of IA Countermeasures for the system. POC may be listed in the POC table. An Information Systems Security Engineer (ISSE) or a System Security Engineer (SSE) is identified for any program delivering Automated Information System applications.	**O&G, Section 5.3.2; DoDI 8500.2 E3.4.4**	**S**
5-14	**5.3.2**	Section describes approach to include appropriate implementation of IA protection for contractor-owned systems.	**O&G, Section 5.3.2;DoDI 8582.01;NIST 800-53 Rev 4**	**S**
5-15	**5.3.3**	Section identifies who is responsible for Software Assurance (SwA) in the PMO.	**DAG Chapter 13.1.1; O&G, Section 5.3.3**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
5-16	**5.3.3**	Section describes how the software will be designed and tested to ensure protection of the system, particularly software supporting Critical Functions/Components and CPI. Section includes discussion of secure design inspection and secure coding practices, e.g., Defense Information Systems Agency (DISA) Application Development Security Technical Implementation Guide (STIG), Software Engineering Institute (SEI) "Secure Coding Standards, etc.	**DoDI 5200.44 Para 4.c.(2) and Enclosure 2 Para 8.b(4); Guidance – generic contract language; DAG Chapter 13.6; O&G, Section 5.3.3, DISA Application STIG, Version 3, Release 5, July 2013**	**C**
5-17	**5.3.3**	Section describes the use of software Automated Static Analysis tools, secure design inspections, and code inspections to inspect for the secure design and code standards established by the program, or states rationale for not implementing the tools and inspections.	**NDAA 2013 Section 933; O&G, Section 5.3.3; DAG Chapter 13.7.3.1.1; 13.7.3.1.2; and 13.7.3.1.3 and SwA Maturity Model, v1.0 Reference Document**	**C**
5-18	**5.3.3**	Section indicates protection of the development environment by providing: (1) a description of who has authority to update or change the development environment; (2) who will be responsible for maintaining a list of cleared U.S. citizens, and foreign nations/foreign nationals that have authority to update or change the environment; (3) the location of these requirements; (5) and the frequency in which they are updated.	**O&G, Section 5.3.3**	**S**
5-19	**5.3.3**	Section describes SwA program activities that are tailored to the program and evolve across the lifecycle.	**O&G, Introduction, pg. 2; DAG Chapter 13.1**	**S**
5-20	**5.3.3; Table 5.3.3-1**	Section and table include evidence that Source code is evaluated with respect to appropriate common weaknesses as evidenced by response in the SwA table.	**DoDI 5200.44 Para 4.c.(4), NDAA 2013 Section 933; O&G, Section 5.3.3, DAG Chapter 13.7.3.1.6**	**C**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
5-21	**5.3.3 Table 5.3.3-1**	Developmental software (CPI, Critical Function/Component) and other developmental SW are evaluated with respect to Common Vulnerabilities and Exposures (CVE), or equivalent, and enumerated in the SwA table, to identify any known vulnerabilities evidenced by discussion. Percentages in table specifies planned versus actual code evaluations.	**DoDI 5200.44 Para 4.c(4); O&G Section 5.3.3;DAG Chapter 13.7.3.1.1; DoDI 5200.39**	**C**
5-22	**5.3.3 Table 5.3.3-1**	Software architectures, environments, designs, and code are evaluated with respect to appropriately selected attack patterns drawn from a Common Attack Pattern Enumeration and Classification (CAPEC) as evidenced by discussion of methods employed and table percentages showing planned versus actual classes of software code evaluations (CPI, Critical Function/Component, and other).	**O&G, Section 5.3.3;DAG Chapter 13.7.3.1.5**	**S**
5-23	**5.3.3 Table 5.3.3-1**	Critical Function/Component software of unknown pedigree is protected and tested and enumerated in the table (e.g., "Operational System/Development Process" rows and "Static Analysis, Design Inspect, and Code Inspect columns.).	**O&G, Section 5.3.3**	**S**
5-24	**5.3.3 Table 5.3.3-1**	Countermeasures are identified in the table for Developmental CPI SW, Developmental Critical Function SW, Other Developmental SW, and commercial off-the-shelf (COTS) (CPI and Critical Function) and NDI SW as protected in the operational system (e.g. Failover Multiple Supplier Redundancy, Fault Isolation, Least Privilege, System Element Isolation, Input Checking/Validation, and Load Key Countermeasures).	**O&G, Section 5.3.3, Table 5.3.3-1**	**S**
5-25	**5.3.3 Table 5.3.3-1**	CWE-compatible tools are used to scan Critical Function/Component software for weaknesses and enumerated in the "Development Process" rows of the table.	**O&G, Section 5.3.3;DAG Chapter 13.7.3.1.3**	**S**
5-26	**5.3.3 Table 5.3.3-1**	Table indicates that the Critical Function/Component software design approach considers design principles to allow system element functions to operate without interference from other elements, as evidenced by enumeration in the "System Element Isolation" column in the "Operational System" rows of the table.	**O&G, Section 5.3.3;DAG Chapter 13.7.3.2.4**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
5-27	**5.3.3 Table 5.3.3-1**	Table, showing planned percentages, lists numeric values greater than or equal to "0" or "None," not a verbal description (e.g., "N/A," "partial," or "unknown.").	**DoDI 5200.44 Para 4.c(4); O&G Table 5.3.3.3-1**	**C**
5-28	**Table 5.3.3-1**	Table indicates protection of the development environment by listing development environment tools in the table.	**NDAA 2013 Section 933, Item (b)(1);O&G, Table 5.3.3-1; DAG Chapter 13.7.3.3**	**C**
5-29	**5.3.4**	Describes the Countermeasures employed to protect Critical Function/Component COTS hardware, software, firmware, of unknown pedigree (i.e., from sources buried in the supply chain). Evidence is provided that Countermeasures are tested and verified.	**O&G, Section 5.3.4**	**S**
5-30	**5.3.4**	Section describes protection of Critical Functions/Components and CPI in the development environment (e.g., in contractor possession) including: analysis of development process vulnerabilities and risks, and plan for process and design mitigations to assure the Critical Function/Component and CPI.	**O&G, Section 5.3.3; DAG Chapter 13.7.3.1 and 13.7.3.3**	**S**
5-31	**5.3.4**	Management of Supply Chain Risks to protect Critical Functions/Components and CPI is described.	**DoDI 5200.44 Para 4.c(2); O&G, Section 5.3.4**	**S**
5-32	**5.3.4**	Section describes protection of sensitive information provided to, maintained at, and received from suppliers and potential suppliers.	**DAG Chapter 13.7.4.2.3**	**S**
5-33	**5.3.4**	Section describes methodology to employ defensive design and engineering protections to protect Critical Functions/Components by reducing unnecessary or unmediated access within the system design.	**O&G, Section 5.3.4; DAG Chapter 13.7.4.2.4**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
5-34	**5.3.4.1**	DoD custom-designed, custom-manufactured, or tailored integrated circuits for a specific DoD military end use (generally referred to as Application Specific Integrated Circuits (ASIC)) shall be procured from a Defense Microelectronics Activity (DMEA) accredited trusted supplier with trusted services, specified to assure a trusted supply chain flow. If due to the program's unique circumstances trusted service cannot be arranged, section describes a risk assessment approach to select and implement alternative countermeasures for mitigating supply chain risk.	**DoDI 5200.44, Para 4.e; CNSSD 505 Section IV, 11; O&G, Section 5.3.4.1**	**C**
5-35	**5.3.4.2**	Section contains a description of: the plan (or references Counterfeit Prevention Plan) to prevent microelectronic counterfeits (of any kind); in Critical Components when items are not obtained from the original equipment manufacturer, original component manufacturer or from an authorized distributor.	**DoDI 5200.44 Para 4.c(3); DoDI 4140.67 Para 3.b and 8.k; DoDI 4140.01, Enclosure 4;10.b.2; O&G, Section 5.3.4.**	**C**
5-36	**Table 5.3.6-1**	Section identifies generic program Countermeasures/security activities	**O&G, Section 5.3.6-1**	**S**
	Section 6	**Other System Security-Related Plans and Documents**	**O&G, Section 6**	
6-1	**6.0**	System security-related plans and documents are identified to include international agreements, systems engineering artifacts, and counter intelligence artifacts.	**O&G, Section 6.0-1**	**S**
6-2	**Table 6.0-1**	Table identifies cooperative arrangements (e.g., Technical Assistance Agreement, Letter of Offer and Acceptance, and Memorandum of Understanding). Table is consistent with Section 8.0.	**O&G, Section 6.0**	**S**
	Section 7	**Program Protection Risks**	**O&G, Section 7.0**	
7-1	**7.0**	Section includes a description of how program protection risks are incorporated into the program's risk management, including: Supply Chain Risk Management (SCRM), supplier threats, IA, exportability, AT, SwA deficiencies, microelectronics (ASIC/FPGA, PCB), etc., when they are identifiable to the supplier as having a DoD end-use.	**DoDI 5200.44 Para4.c, 4.d; O&G, Section 7.0**	**C**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
7-2	**7.0**	When threat reports have been received, section provides evidence that all-source intelligence analysis of suppliers of critical components is used to inform risk management decisions.	**DoDI 5200.44 Para 4.b**	**C**
7-3	**7.0**	Section includes a risk cube and mitigation plan for top program protection risks.	**O&G, Section 7.0**	**S**
7-4	**7.0**	If there are limited suppliers and malicious threat information is not available, medium or medium-high threat is assumed and is used to inform the Level I Critical Functions/ Components risk assessment.	**DoDI 5200.44 Para 4.a-e.; O&G, Section 7.0**	**S**
7-5	**7.0**	The supply chain malicious insertion threats (generic or specific) including software/firmware and vulnerabilities have been used to assess risk for the Level I and Level II Critical Functions/Components risk assessment.	**DoDI 5200.44 Para 4.a-e.; O&G, Section 7.0**	**C**
7-6	**7.0**	Section confirms the program identifies, documents, and reassesses risks for SCRM (Including Trusted Systems and Networks (TSN), IA, SwA, microelectronics (FPGA, ASIC, PCB, etc.)) with rationale and risk mitigation or risk acceptance, before each SETR and milestone decision review. Section specifically describes mitigation applied to microelectronics.	**DoDI 5200.44 Para 4.c, 4.d; O&G, Section 7.0**	**C**
7-7	**7.0**	Section describes the method used to incorporate the assessed criticality, threats, and vulnerabilities into the risk determination.	**O&G, Section 7.0**	**S**
7-8	**7.0**	PMO has developed a risk mitigation plan for all DIA TAC Report results with a high threat or critical report. The mitigation approach is documented in a POA&M, or risk acceptance has been documented with rationale.	**DoDI 5200.44 Para 1.d and 4.a-e, Enclosure 2 Para 8; O&G, Section 7**	**C**
	Section 8	**Foreign Involvement**	**O&G, Section 8.0**	
8-1	**8.0**	Section summarizes international activities through responses to all the questions in the first four bullets in O&G Section 8.0.	**O&G, Section 8.0; DTM 11-053**	**C**
8-2	**Table 8.0-1**	Table aligns with acquisition documents and is complete.	**O&G, Table 8.0-1**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
8-3	**8.0/8.1**	Section provides a complete response to all the questions listed in O&G for Section 8.1. Foreign involvement and defense exportability planning are summarized in Sections 8.0 and 8.1 to indicate the potential exposure and planning to protect CPI in export variants. For designated DEF pilot programs, section includes description of plan to identify, develop, and incorporate technology protection for the purpose of enhancing or enabling each system's exportability.	**O&G, Section 8.1; NDAA FY 2011, Section 243**	**C**
	Section 9	**Process for Management and Implementation of PPP**	**O&G, Section 9.0**	
9-1	**9.1**	Section addresses audits and inspections.	**O&G, Section 9.1**	**S**
9-2	**9.1**	Section describes the incorporation of program protection planning considerations into SETR criteria as defined in the SEP. Section includes references to SEP sections.	**O&G, Section 9.1**	**S**
9-3	**9.2**	Section confirms the PMO has updated the PPP for each SETR, including but not limited to the areas of CPI, AT, Defense Exportability Features, SCRM, TSN, IA, Vulnerability Assessments, Threat Assessments, and Countermeasure / mitigation selection and implementation.	**DoDI 5200.44 Para 4.a, 4.c; O&G, Section 9.2; NDAA FY 2011 Section 243; DoDI 5200.39; DAG Chapter 13**	**C**
9-4	**9.3**	Section describes Countermeasures and implementation plans, including how supply chain and malicious insertion penetration, blue team, or red team testing are incorporated into the verification and validation criteria, process, and procedures for custom and commodity hardware and software.	**DoDI 5200.44 Para 4.c.3 and 4.c.4; O&G, Section 9.3**	**C**
9-5	**9.3**	Section describes how the program will integrate system security requirements testing into the overall test and evaluation strategy.	**O&G, Section 9.3**	**S**
9-6	**9.4**	Section describes the program protection approach during Sustainment with respect to periodic (every 12-18 months) and event-driven (tech refresh, enhancement) PPP analysis and PPP updates. Section should link to the relevant Life Cycle Sustainment Plan (LCSP) language.	**O&G, Section 9.4**	**S**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
9-7	**9.4**	Section confirms that the program updates and counters program protection supply chain, IA, and other risks throughout the entire system lifecycle (up to system disposal) periodically (12-18 months), or event-driven (tech refresh, enhancement). Section should be consistent with the LCSP.	**O&G, Section 9.4; DoDI 5200.44, Para 4.c; DAG Chapter 2.3.12.4**	**S**
	Section 10	**Process for Monitoring and Reporting Compromises**	**O&G, Section 10.0**	
10-1	**10.0**	Section summarizes the PMO's plan for responding to system compromise, including compromise resulting from supply chain, IA, exfiltration, and compromise of CPI.	**O&G, Section 10.0**	**S**
10-2	**10.0**	Section defines supply chain compromise or exploit.	**O&G, Section 10.0**	**S**
	Section 11	**Program Protection Costs**	**O&G, Section 11.0**	
11-1	**11.2**	Table includes Acquisition and Systems Engineering Protection Costs, SCRM and IA cost, and other cost above National Industrial Security Program Operating Manual requirements.	**O&G, Section 11.2; DAG Chapter 8.4.6.7 and 13.12.2**	**S**
	Appendices	**Appendices**	**O&G, Appendices**	
C-1	**C**	Appendix confirms the Criticality Analysis is updated for each PPP submission to reflect the updates and elaboration to the level of the system design. Critical Functions are allocated to subsystems, subassemblies, and components as each element is defined in the design.	**DoDI 5200.44 Para 1a; O&G Appendices**	**C**
C-2	**C**	Appendix documents Critical Functions to include: functions with unmediated access to the Critical Functions, functions that Critical Functions depend upon, and defensive functions.	**DoDI 5200.44, Glossary Part II; O&G, Section 2.2-1**	**S**
D-1	**D**	Appendix confirms one of the following conditions has been met: (1) ATEA concurs with the approved AT Plan; (2) ATEA has provided written concurrence with a draft AT Plan; or (3) ATEA has provided written concurrence indicating that no AT Plan is required at this stage of the program. *AT Plan is due for ATEA review no later than 105 days prior to each Milestone.*	**DoDI 5200.39**	**C**

Evaluation Criteria Number	Program Protection Plan (PPP) Requirements		Policy and Guidance References	Criteria
E-1	**E**	Appendix confirms one of the following conditions has been met: (1) DoD CIO has approved the Acquisition IA Strategy (AIAS); (2) DoD CIO has provided concurrence with a draft AIAS; or (3) DoD CIO has provided written concurrence indicating no AIAS is required at this stage of the program.	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices**	**C**