



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 240-110-42*

FEB 24 2014

SECURITY

Program Protection

1. **Purpose.** This Instruction prescribes policy and assigns responsibility for program protection. It also provides guidance on a Program Protection Plan (PPP).
2. **Applicability.** This Instruction applies to DISA activities.
3. **Authority.** This Instruction is published in accordance with the authority contained in Interim DoD Instruction 5000.02, Operation of the Defense Acquisition System, 25 November 2013, and DoD Instruction 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense, 16 July 2008.
4. **Definitions.** Definitions are provided in enclosure 1.
5. **Policy.**
 - 5.1 Program protection will be institutionalized within the Agency as an integral part of the day-to-day acquisition life-cycle process.
 - 5.2 A PPP will be created, maintained, updated, and executed for each individually named program within a Program Management Office (PMO) and throughout each program's acquisition life cycle.
6. **Responsibilities.**
 - 6.1 **Manpower, Personnel, and Security (MPS) Chief, Security Division (MPS6).** The Chief, MPS6, as the Senior Intelligence Officer (SIO) for DISA, will:
 - 6.1.1 Oversee program protection for the Agency.
 - 6.1.2 Update Principal Directors, Directors, Commanders, and Chiefs of major organizational elements on the progress and status of program protection within the Agency.
 - 6.1.3 Oversee the implementation of PPPs throughout the Agency.
 - 6.1.4 Provide program protection training and education.
 - 6.1.5 Provide timely, effective response to requests for guidance and assistance by the Program Management Executives (PMEs), Program Managers (PMs), and Action Officers (AOs).

6.1.6 Assist PMOs by reviewing their PPPs, when requested.

6.2 Principal Directors, Directors, Commanders, and Chiefs of Major Organizational Elements. These individuals will:

6.2.1 Ensure program protection within their organizations is managed in accordance with this Instruction.

6.2.2 Ensure PMOs create, maintain, update, and execute a PPP for each individually named program within their purview and throughout the acquisition life cycle.

6.2.3 Evaluate the viability and effectiveness of a PPP of their PMOs annually and report their assessments and follow-up actions to MPS6.

7. Duties.

7.1 Lead Counterintelligence (CI) Agent. The Lead CI Agent, located in MPS6, will:

7.1.1 Assist PMOs with the development and/or review of their operations security (OPSEC) planning as a subset of their PPPs.

7.1.2 Assist PMOs with identification of their Critical Program Information (CPI), mission-critical functions, and components as a subset of their PPPs.

7.1.3 Develop a Counterintelligence Support Plan (CISP) for each PPP.

7.1.4 Provide CI support, as required, to include threat assessments, Supply Chain Risk Management (SCRM) assessments, awareness training, foreign travel briefings and debriefings, and foreign contact briefings.

7.2 Program Managers (PMs) and Action Officers (AOs). A PM and AO of a program that develops systems for use on or is associated with DoD networks will:

7.2.1 Develop and implement a PPP during the planning portion of the acquisition.

7.2.2 Ensure CPI is identified to aid in protection during Requests for Information (RFIs) and Request for Proposals (RFPs).

7.2.3 Evaluate program development and update CPIs, as needed.

7.2.4 Ensure SCRM is captured as part of the PPP to provide for evaluation of components connected to DoD systems.


7.2.5 Ensure contractors submitting proposals include a security plan that addresses how the contractor will protect classified and sensitive information as called for within the PPP.

8. Program Protection Plan (PPP). A PPP will ensure program technology, mission-critical functions, components, and intellectual property are properly and prudently protected to include sensitive but unclassified information and data which, if compromised or aggregated with other compromised information, could permit an adversary to affect DoD systems and capabilities. The creation of a PPP serves as the impetus behind a deliberate and disciplined assessment of what needs to be protected and how optimal protection will be afforded given available time and resources. A PPP will be classified by content in accordance with the applicable regulations and instructions. At a minimum, the Agency PPP will include the components identified in enclosure 2.

8.1 Maintaining an end-to-end system view is critical when developing and executing a PPP. Additionally, external, interdependent, or government-furnished components that may exist outside of the purview of the PM must also be considered for inclusion in the PPP. The PPP is to be a useful, easy-to-understand reference for managing the full spectrum of program and system security activities. The PPP is to be right-sized to the acquisition. Accordingly, it is to contain information and guidance that anyone working on the program can easily reference, comprehend, and utilize to carry out program protection duties and responsibilities.

8.2 At Key Decision Point A in the acquisition process, it is possible that not all of the required program protection information will be available. At a minimum, a PPP for Key Decision Point A is to include (1) candidate CPI and potential protection countermeasures; (2) identification of the OPSEC Essential Elements of Friendly Information (EEFI) and compilation of the OPSEC Critical Information List (CIL); (3) a Security Classification Guide (SCG), if applicable; and (4) an information assurance (IA) strategy. The PPP for Key Decision Point B is to reflect a complete and comprehensive document.

2 Enclosures a/s



FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

*This Instruction must be reissued, canceled, or certified current within 5 years of its publication date. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.

OPR: MPS – disa.meade.mps.mbx.special-security-office-group-mailbox@mail.mil

DISTRIBUTION: P

Enclosure 1

DEFINITIONS

Acquisition Information Assurance Strategy. Strategy developed by the Program Manager ((PM) to help the program office organize and coordinate its approach to identifying and satisfying information assurance (IA) requirements consistent with DoD policies, standards, and architectures.

Antitamper (AT) Measures. Systems engineering (SE) activities intended to prevent and/or delay exploitation of critical technologies in U.S. systems. These activities involve the entire life cycle of systems acquisition including research, design, development, testing, implementation, and validation of the antitamper measures.

Counterintelligence (CI). Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.

Counterintelligence Support Plan (CISP). A formally coordinated action plan for counterintelligence (CI) support to protect research and technology at specific DoD research, development, test, and evaluation facilities and acquisition programs. The plan addresses key aspects of the installation, the activity or program, and the nature of the CI activities to be employed.

Critical Information List (CIL). An OPSEC term. A compiled list containing specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

Critical Program Information (CPI). Those program elements which, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; and enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

Essential Elements of Friendly Information (EEFI). An OPSEC term. Within the context of "friend or foe," these are specific pieces of information regarding friendly (i.e., U.S.) intentions, capabilities, and activities which are likely to be sought by our foes (i.e., our enemies/competitors).

Horizontal Protection Plan. A planning process that determines if critical defense technologies, to include Critical Program Information (CPI), associated with more than one research, development, and acquisition (RDA) program, are protected to the same degree by all involved DoD activities.

Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Operations Security (OPSEC). An analytic process used to deny adversary information (generally unclassified) concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations.

Program Protection. Integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition life cycle.

Program Protection Plan (PPP). A plan that assists programs to ensure that their technology, components, and information are adequately protected.

Security Classification Guide (SCG). A document that details how information will be classified and marked in support of an acquisition program. It is the written record of an original classification decision or series of decisions regarding a system, plan, program, or project. An SCG addresses each Critical Program Information (CPI), as well as other relevant information requiring protection, including export-controlled information and sensitive but unclassified information.

Supply Chain Risk Management (SCRM). A discipline that addresses the threats and vulnerabilities of commercially acquired information and communications technologies within and used by government information and weapon systems. Through SCRM, systems engineers can minimize the risk to systems and their components obtained from sources that are not trusted or identifiable as well as those that provide inferior material or parts.

Enclosure 2

COMPONENTS OF A PROGRAM PROTECTION PLAN (PPP)**Operational Security (OPSEC) Plan**

The OPSEC plan safeguards sensitive but unclassified information and data. The OPSEC Essential Elements of Friendly Information (EEFI) and Critical Information List (CIL) is to be included in an enclosure to the PPP.

Methodology to Identify and Safeguard Critical Program Information (CPI), Mission-Critical Functions, and Components

The CPI is to be included as an enclosure to the PPP.

Counterintelligence Support Plan (CISP)

The CISP outlines and describes the counterintelligence (CI) support to be provided to research and development facilities, research development and acquisition (RDA) programs with CPI, and CPI resident at cleared contractor facilities. A CISP is coordinated with and approved by the RDA Director, Program Management Office (PEO), or Program Manager (PM), as appropriate, and is to be included as an enclosure to the PPP.

Horizontal Protection Plan

The Horizontal Protection Plan determines if critical DoD technologies, to include CPI, associated with more than one RDA program, are protected to the same degree by all involved DoD activities.

Acquisition Information Assurance (IA) Strategy**Security Classification Guide (SCG)****Antitamper (AT) Measures****Supply Chain Risk Management (SCRM) Plan****Program Protection Costs Estimate****Process to Manage and Implement the PPP****Process for Monitoring and Reporting Compromises**