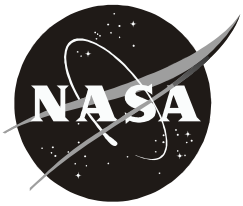

National Aeronautics and
Space Administration

**CxP 70070-ANX05**

**BASELINE**

**RELEASE DATE: JUNE 17, 2008**

# CONSTELLATION PROGRAM, PROGRAM MANAGEMENT PLAN, ANNEX 5: SECURITY MANAGEMENT PLAN

## REVISION AND HISTORY PAGE

| Status | Revision No. | Change No. | Description | Release Date |
|---|---|---|---|---|
| Baseline | - | - | Baseline (Reference CxCB C000249, dated 06/11/08) | 06/17/08 |

# Table of Contents

## Section Page

## Figures



## Tables

## Appendix

# 1.0 Introduction

On January 14, 2004, the President of the United States directed the National Aeronautics and Space Administration (NASA) to embark on a robust space exploration program to advance the nation's scientific, national security, and economic interests. To support this vision, the Constellation Program (CxP) developed a security approach that ensures uncompromised scientific and engineering capabilities and space technologies by providing security measures, interfaces, and strategies to the projects that encompass the CxP architecture.

## 1.1 Purpose

CxP 70070, Constellation Program, Program Management Plan, Annex 5: Security Management Plan (SMP) identifies and defines the security goals and objectives of the Program, Program relationships, roles and responsibilities, the environment within which the security program operates, and the baseline security commitments of the program. This includes identifying the full range of security and technology protection requirements for the program and each constituent project which includes export control, physical and mission essential infrastructure (MEI) security, industrial and information security, program security, personnel security, communications security (COMSEC), counterintelligence (CI) and counterterrorism (CT) support, information assurance (IA), disaster planning, and information technology (IT) security.

## 1.2 Scope

This SMP applies to all CxP projects, elements, contractors, activities, and locations. It describes the integrated approach for security and technology protection. It also outlines the safeguards, protection mechanisms, and controls to ensure uniformed and effective implementation of security and protective services across the CxP in accordance with applicable requirements and directives. Any security management plans (Level III and below) or work instructions generated by the projects are subordinate to this SMP and reference this document.

## 1.3 Authority

The NASA Office of Primary Responsibility (OPR) for developing and implementing this document is the Constellation (Cx) Program Planning and Control (PP&C) Office in accordance with NPR 1600.1, NASA Security Program Procedural Requirements.

## 1.4 Configuration Control

Updates to this SMP are in accordance with the CxP configuration management control process and are made as the Cx Program proceeds through design, development, production, integration, test and deployment. Proposed changes to this document and any related documents are submitted by a program change request (CR) to the Cx Security Control Board {TBR} and Cx Control Board (Cx CB) for consideration and disposition.

## 1.5 Overview

Overall responsibility for day-to-day security management has been delegated by the Cx Program Manager (PM) to the Cx PP&C, Technology Protection Officer (TPO). See Figures 1.5-1 (Organization Overview) and 1.5-2 (Constellation Program Security Organizational Structure) in this SMP. To meet this responsibility, PP&C leverages support and resources from NASA Institutional Protective Services Division personnel and the Exploration Systems Mission Directorate (ESMD) Technology Protection Working Group (TPWG) established to advise and assist in developing and implementing a risk-based security and technology protection program.

This SMP is consistent with NPR 1600.1 and NPR 7120.5D, NASA Space Flight Program and Project Management Requirements. This SMP governs how the program and projects that make up the CxP architecture are secured throughout the program life cycle. The contents of this document are synopsized as follows:

Section 2.0, Documents, identifies applicable and reference documents.

Section 3.0, Security Approach, describes the approach to security and technology protection for the CxP.

Section 4.0, Technology Transition, describes the technology transition strategies for the program.

Section 5.0, Roles and Responsibilities, describes the roles and responsibilities of key personnel.

Section 6.0, Security and Technology Protection Requirements, describes the required processes for all protection disciplines.

Section 7.0, Security Awareness and Technical Training describes the training for security and technology protection.

Section 8.0, Reporting, describes the reporting of security and technology protection information

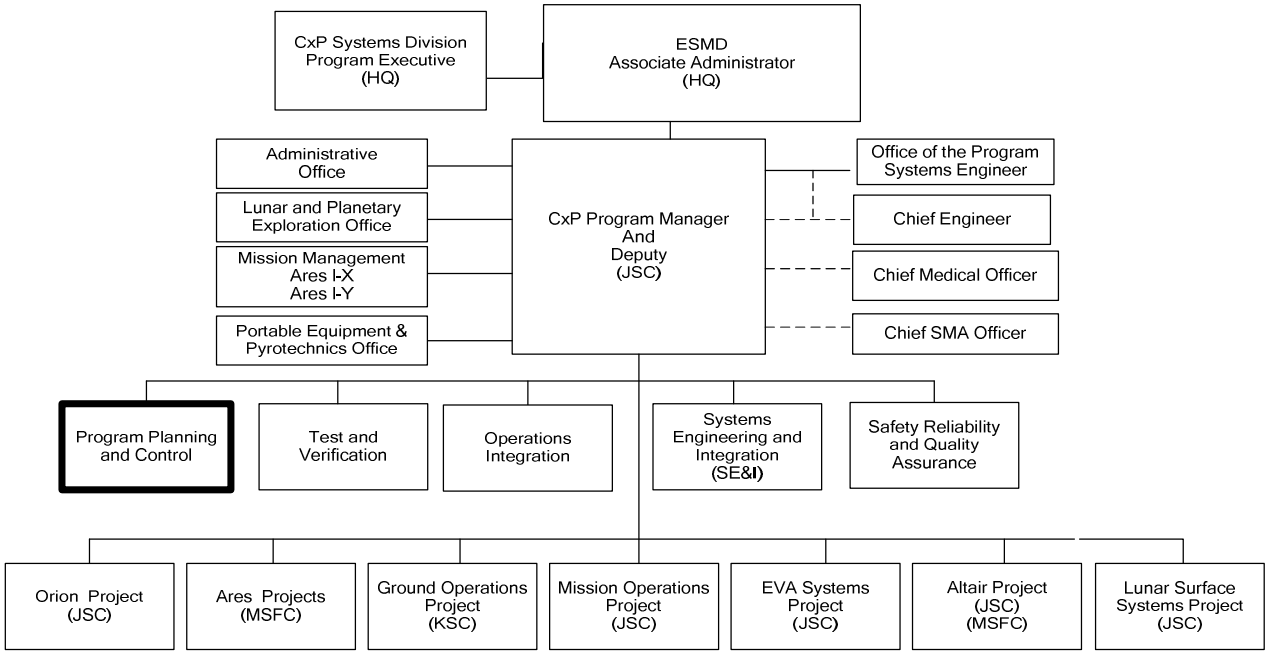


**Figure 1.5-1, Organization Overview**

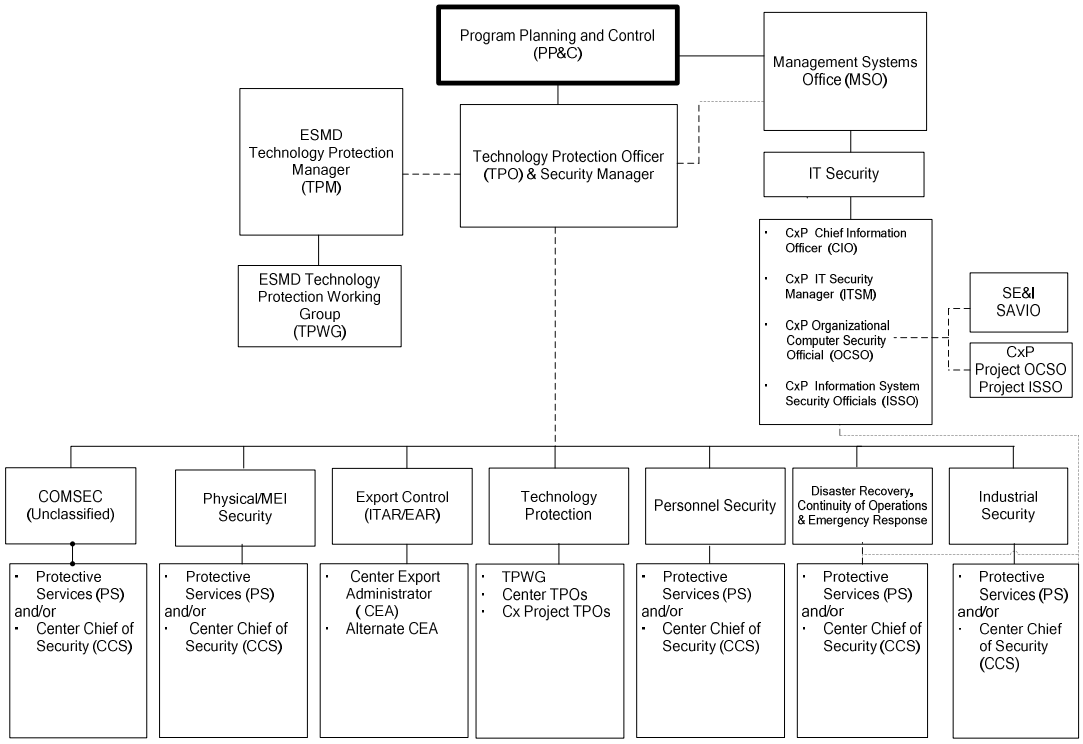


**Figure 1.5-2, Constellation Program Security Organizational Structure**

## 1.6 Security Documentation Tree

CxP 70070, Constellation Program, Program Management Plan, Annex 5: Security Management Plan is reflected on Figure 1.6-1. It represents the program document structure. The structure of the security management function is described in detail in the following program documents:

CxP 70070, Constellation Program, Program Management Plan
CxP 70070-ANX05, Security Management Plan

CxP 70070-ANX05-03 (SMP Book 3): CxP Disaster Recovery, Continuity of Operations, and Emergency Response Plan – Defines the processes for emergency and contingency operations.

CxP 70070-ANX05-04 (SMP Book 4): CxP Technology Protection Program Plan (TPPP) – Defines the key technology protection processes - e.g., mission critical information (MCI) and/or mission essential infrastructure (MEI) assessments, threat

and vulnerability assessment (TVA), risk analysis, countermeasures selection, etc., and documents the Program Manager's (PM) validated list of MCI or MEI.

CxP 70070-ANX05-05 (SMP Book 5): CxP Information Technology (IT) Security Threat and Vulnerability Assessment (TVA) Process Plan (PP) -- captures inputs from external subject matter experts/organizations relative to validated threats and vulnerabilities, provides NASA a more comprehensive and accurate assessment of the security risks against CxP IT Systems, and allows for an informed basis on which to select/modify security controls.

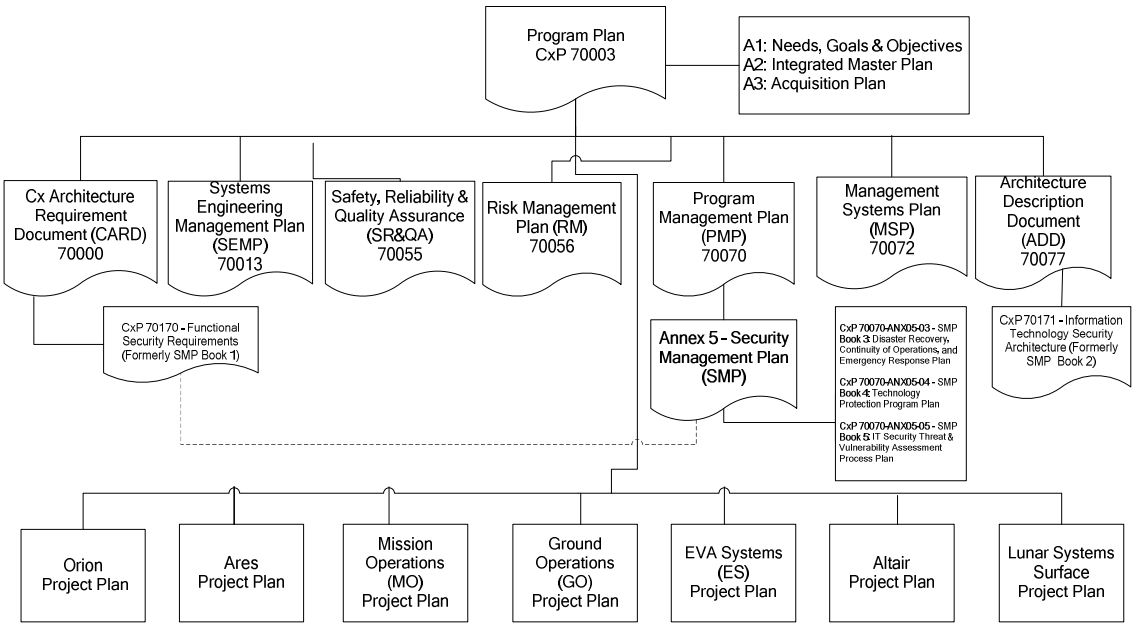


**Figure 1.6-1, Constellation Program Top-Level Document Tree**

# 2.0 Documents

The federal and agency directives and documentation listed in the following subsections apply to all CxP element locations until and unless they are superseded by guidance released by the appropriate agency or Center level office.

## 2.1 Applicable Documents

- DoD 5220.22M, National Industrial Security Program Operating Manual (NISPOM), February 2006

- Homeland Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization and Protection, December 17, 2003
- HSPD 12, Personal Identity Verification/Validation (PIV), August 12, 2004
- NPD 1600.2D, NASA Security Policy
- NPR 1371.2A, Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities w/Change 1
- NPR 1040.1, NASA Continuity of Operations (COOP) Planning Procedural Requirements
- NPR 1600.1, NASA Security Program Procedural Requirements
- NPR-1600-1, NASA Interim Directive, Personal Identify Verification (PIV) Policy and Procedures
- NPR 1620.2, Physical Security Vulnerability Risk Assessments
- NPR 1620.3, Physical Security Requirements for NASA Facilities and Property
- NPR 1620.4 (Draft 5), National Security Systems (COMSEC) {TBR}
- NPR 1660.1, Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirements
- NPR 2190.1, NASA Export Control Program
- NPR 2200.2B, Requirements for Documentation, Approval, and Dissemination of Scientific and Technical Information
- NPR 2800.1, Managing Information Technology w/Change 1
- NPR 2810.1A, Security of Information Technology
- NPR 2830.1, NASA Enterprise Architecture Procedure
- NPR 7120.5D, NASA Space Flight Program and Project Management Processes and Requirements
- NPR 8715.2, NASA Emergency Preparedness Procedural Requirements Plan
- CxP 70070-ANX05-03 (SMP Book 3), CxP Disaster Recovery, Continuity of Operations, and Emergency Response Plan {TBR}

- CxP 70070-ANX05-04 (SMP Book 4), CxP Technology Protection Program Plan (TPPP) {TBR}

- CxP 70070-ANX05-05 (SMP Book 5), CxP Information Technology (IT) Security Threat and Vulnerability Assessment (TVA) Process Plan (PP) {TBR}

## 2.2 Reference Documents

- CxP 70003, Constellation Program Plan
- CxP 70056, Constellation Program Risk Management Plan
- CxP 70070, Constellation Program, Program Management Plan
- CxP 70170, Functional Security Requirements (formerly Book 1)
- CxP 70171, Information Technology Security Architecture (formerly Book 2)
- ESMD-SBUWI1, ESMD Sensitive But Unclassified (SBU) Work Instruction
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- Space Operations Mission Directorate and ESMD Human Space Flight Transition Plan (TCB-001, November 12, 2006)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-100, Information Security Handbook: A Guide for Managers
- 14 CFR 1205, Subpart 10

# 3.0 Security Approach

The CxP Technology Protection Program (TPP) is established to define, develop, and ensure that security and protective measures are implemented throughout the CxP. The major focus areas to be addressed throughout the life cycle of the program are system security, IT security and information assurance, and technology protection. This approach aids in identifying security risks in system designs,

acquisitions, or modifications early, thereby minimizing security costs, vulnerabilities, and possible loss or compromise of NASA MCI and technology.

The CxP projects use this SMP and its associated books as the baseline policy and procedural documents to establish a project security and technology protection program that aligns closely with the CxP and ESMD expectations and direction.

The CxP TPO, Project TPOs, Organizational Computer Security Official (OCSO), and industry partners participate on agency-wide security teams or at agency-wide security forums to ensure the provision of products and services that meet current program needs, while adhering to federal laws, agency directives, and agency and Center requirements.

ESMD chartered the TPWG to coordinate and status technology protection, system security engineering (SSE), IT security, information assurance, and general security-related activities across the CxP and other ESMD programs and projects. The TPWG is responsible for ensuring that key interfaces between the program, project offices, and all Government and contractor organizations involved in protection activities are provided. NPR 1600.1 provides for the assignment of management security responsibilities and establishes agency-wide security program implementation requirements set forth in NPD 1600.2D, NASA Security Policy.

The SMP Book 4 (CxP TPPP) documents the methodology used to identify the CxP MCI and analyze the MCI-associated system security vulnerabilities, countermeasures, and residual risk in the TVA. The MCI identification effort is both technology- and systems-driven, but the countermeasure selection effort is threat-driven. The CxP is confronted by three levels of protection: classified information protection, where appropriate; Sensitive But Unclassified (SBU) protection; and MCI protection. CxP information is released to the public after an appropriate review in accordance with NASA and CxP public release guidelines.

## 3.1 Risk Management

The CxP TPO coordinates with the TPWG, Project TPOs, and OCSO to implement Continuous Risk Management (CRM) strategies and techniques for all security and technology protection disciplines as described in Section 1.1 of this SMP.

The Cx Program Manager, with assistance from the TPWG, conducts a tailored TVA to validate existing and emerging threats directed at systems and technologies. Appropriate risk management processes to identify and determine the threat and

level of associated risk are performed and are documented in the SMP Book 4 (TPPP). The candidate risks are submitted to the appropriate level risk management database (Level I, II, or III) for approval. Candidate risks may be evaluated throughout the program by using the established review process to ensure continuity and conformity based on NASA Headquarters (HQ) ESMD and Office of Security and Program Protection (OSPP) threat analysis and risk management practices.

## 3.2 Constellation Technology Protection Program

The CxP personnel ensure the protection of all key assets and technologies, including MCI and MEI that are identified within the CxP. The ESMD Technology Protection Manager (TPM) and CxP TPO coordinate with other cognizant Government intelligence agencies regarding threats and develop plans to mitigate those risks to the maximum extent possible. The approach to identify security risks follows the program's risk management process (CxP 70056, Risk Management Plan). The rationale proceeds from the following:

- The CxP provides protection mechanisms and processes in compliance with agency and directorate program protection policies.
- The CxP makes effective use of its resources, existing management processes, and organizational infrastructure.

  Note: Planning and budget activities are incorporated into the workflow and work breakdown structure (WBS) as part of individual program or project level contracts.
- CxP protection activities address major aspects of the program to prevent compromise or propagation of vulnerabilities across major system interfaces and boundaries. These measures ensure system robustness and the ability to operate consistent with the policies, practices, recommendations, and guidelines of U.S. National Space Policy.

CxP management coordinates with the OSPP, ESMD Directorate Integration Office (DIO), and the TPWG for advice and guidance in implementing program-related protection activities which are defined in the SMP Book 4 (TPPP). The CxP, ESMD, and OSPP operate as an integrated organization responding to priorities, functional criticalities, and changing resource demands. The focus is on mission support and enhanced performance while reducing duplications of effort. Regionally, the Center Chief of Security (CCS) and TPOs tailor operations to local program and project needs, permitting flexibility for addressing shifts in security emphasis. They also

tailor operations to respond to varying protection needs or potential protection strategy changes.

## 3.3 Constellation Information Technology (IT) Security Program

The Cx IT Security Program is developed in accordance with NPR 2810.1A, Security of Information Technology, and uses National Institute of Standards and Technology (NIST) Special Publication 800-100, Information Security Handbook: A Guide for Managers, as guidance. The CxP also adheres to the Agency IT Governance Model.

## 3.4 Constellation System Security Engineering

System security engineering involves security planning and risk mitigation, accreditation services, disaster recovery and continuity of operations, security testing and evaluation, and security architecture (engineering and management). The CxP uses the principles of system security engineering to ensure that security is properly designed into all systems from the start. Primary focus is placed on the critical components needing protection, cost effective security countermeasure designs, and budget planning to ensure that funds are available to implement countermeasures.

System security involvement ensures that the CxP addresses appropriate and consistent protection countermeasures for space launch programs/vehicles throughout the life-cycle of the program. The TPWG provides security and information assurance services to assist the CxP with program management, systems engineering, information technology, and risk management (identification, assessment, acceptance, and mitigation methods). Selected countermeasures are based on system security trade studies of relevant factors and supporting data such as risk level (including impact and probability), available alternatives, cost factors, trends, historical information, environments, and directives. Security requirements are documented and selected countermeasures implemented.

## 3.5 Constellation Protection Strategies

The CxP TPP establishes an environment in which program personnel assist in maintaining essential security of the most critical CxP information and technologies. NASA's technological advantage is maintained and secured by enhancing the protection of the most critical MCI assets.

As new requirements to security operations expand, support is required for flight engineering, maintenance, and operations of secure facilities and systems through

the implementation of, and adherence to NASA site-specific requirements, Federal Information Security Management Act (FISMA), and the SMP.

### 3.6 Disaster Recovery, Continuity of Operations, and Emergency Response

In accordance with NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedural Requirements NPR 8715.2, NASA Emergency Preparedness Plan Procedural Requirements, and SMP Book 3 (Disaster Recovery, Continuity of Operations, and Emergency Response Plan), the range and scope of potential crises and specific response actions, timing of notifications and actions, and responsibilities of key individuals are defined.

The CxP leverages Center procedures for emergency preparedness and COOP depending on where the team member is physically located. Team members must follow their Center procedures for these types of directives.

## 4.0 Technology Transition

The CxP 70003, Program Plan, and CxP 70070, Program Management Plan, are applicable through the acquisition of all program systems and elements until they are transitioned and accepted by the Space Operations Mission Directorate (SOMD).

The technology transition strategies are defined in the Space Operations Mission Directorate and ESMD Human Space Flight Transition Plan (TCB-001, November 12, 2006).

The CxP, with assistance from ESMD and OSPP, facilitates the successful transition of the Space Shuttle Program (SSP) and International Space Station Program (ISSP) technologies and resources to Cx systems and ensures cross-organizational integration in accordance with the Human Space Flight Transition Plan. The CxP ensures that each contractor security organization acts strategically as a single entity at multiple operating locations, while maintaining the flexibility to address local program requirements effectively.

CxP information and data that transit across these systems and platforms are assessed and protected based upon risk, threat, and vulnerability assessment. The CxP adheres to the agency's information assurance (IA) policy as it applies to security management.

Plans for integration of new NASA protection requirements into the CxP are developed and executed as needed. Protection requirements transitioned into the CxP involve absorbing or integrating security responsibilities or both, and activities from other contracts such as these are phased under the CxP. As the CxP authorizes specific protection transitions, respective plans and schedules are documented and executed.

# 5.0 Roles and Responsibilities

The HQ OSPP and Office of Chief Information Officer (OCIO) provide policy, oversight, and support to the ESMD. The ESMD chartered the TPWG to provide guidance, assistance, and oversight of the CxP TPP. Designated CxP representatives are core members of the TPWG.

The Cx PM has overall responsibility for ensuring effective implementation of this SMP and relies on the OSPP, OCIO, CxP TPO, each CCS or Center TPO, and the TPWG subject matter experts for advice and assistance**.** Figure 5.0-1 is a revised version of the ESMD Technology Protection Process Assurance Map that depicts high level interfaces between ESMD, OSPP, and TPWG.

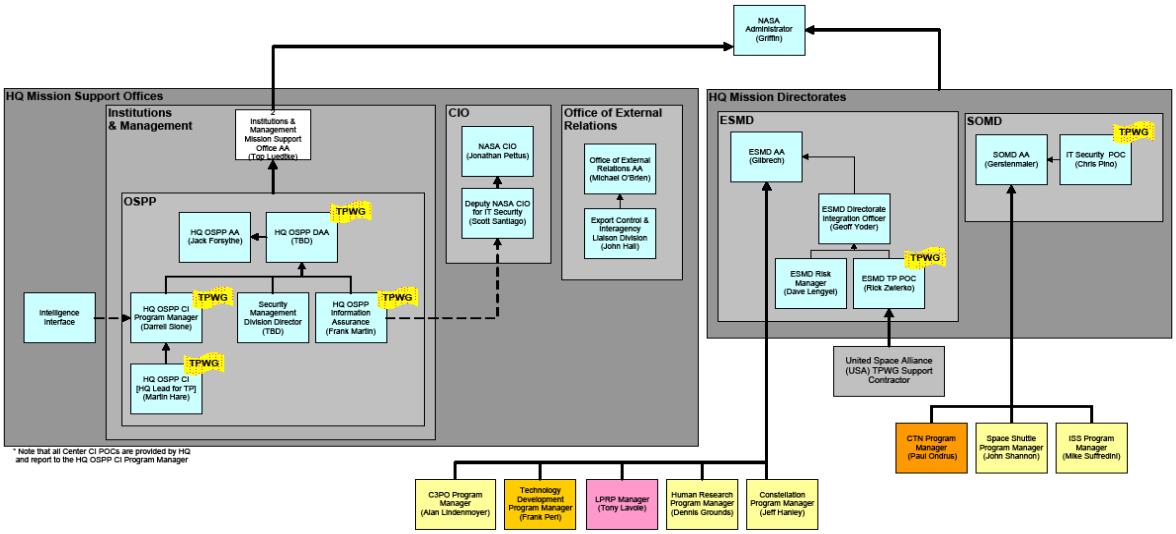


**Figure 5.0-1, ESMD Technology Protection Process Assurance Map**

### 5.1 ESMD Associate Administrator

The ESMD Associate Administrator (AA) has full responsibility and authority for the operations and conduct of the CxP. The ESMD AA directs the implementation and ensures compliance with the TPPP established by the ESMD DIO through partnering efforts with the OSPP. The CxP leverages the existing Center Chiefs of Security to fulfill specific roles identified in NPR 1600.1.

### 5.2 ESMD Technology Protection Manager (TPM)

The ESMD TPM or designee is appointed by the ESMD AA and is responsible for coordinating day-to-day directorate-level (Level I) technology protection planning and implementation efforts. The TPM established the ESMD TPWG. The Community of Practice (CoP) was established as a secure communication tool on which multi-disciplined stakeholders share information, discuss, status, and resolve issues and concerns relative to security and technology protection. Designees from all performing organizations are invited to participate in the ESMD CoP.

### 5.3 Cx Program Manager (PM)

The Cx PM provides overall direction and guidance for the program to ensure compliance and uniformity with agency policies, procedures, and priorities, as well as other applicable government regulations. The CxP Office provides the management of and the integration between the numerous Cx project offices across the agency. The Cx PM is the responsible Risk Acceptance Authority (RAA) for validating MCI, has signature authority for the SMP, and directs its implementation across the CxP.

### 5.4 CxP Project Manager

The CxP Project Managers are responsible to the Cx PM for execution of all activities required to meet NASA's program-level requirements and security objectives as defined in the Cx Program Plan.

### 5.5 CxP Technology Protection Officer (TPO)

The CxP TPO is appointed by the Cx PP&C Manager and is responsible for implementing and ensuring compliance with security, export control, and technology protection requirements. The CxP TPO is the PP&C Assistant for Security Management and a member of the TPWG with the knowledge and authority to provide input and make protection-related decisions on behalf of the CxP and is the primary interface to the ESMD TPM and TPWG regarding the CxP TPP.

### 5.6 CxP Chief Information Officer (CIO)

The CxP CIO is a senior-management appointed official to represent his/her respective organization and collaborate with the NASA CIO in establishing IT policies and standards. The CxP CIO reports to the CxP PP&C manager.

The CxP CIO performs the "CIO" role as defined in NPR 2810.1A and in Section 2.2 of NPR 2800.1, but within the scope of the CxP instead of NASA, HQ, or a NASA Center . The CxP CIO is responsible for Enterprise Architecture in accordance with NPR 2800.1 and 2830.1, NASA Enterprise Architecture Procedure. The CxP CIO is also responsible for all CxP owned and/or operated systems, including the security of those systems. The CxP CIO supports and coordinates with the CxP PM and the JSC Center CIO to ensure appropriate planning, resourcing, and execution of IT security functions performed by the CxP.

The CIO grants the ITSM the authority to determine when an IT security incident is placing NASA's missions, its customers, its reputation, or its assets in immediate jeopardy to a degree that the program must exercise its responsibility to unilaterally control or terminate actions. The CxP ITSM works closely with the Center CIO, CCS, Office of Inspector General (OIG), CxP OCSO, and Project ISSOs to ensure coordination of required actions.

### 5.7 CxP Information Technology Security Manager (ITSM)

The CxP ITSM supports the CxP CIO to ensure compliance with NASA policies, requirements, and directives from the CxP CIO. The CxP ITSM also develops any additional policies and guidance to be approved by the CxP CIO. Additionally, the CxP ITSM tracks the status of system security plans assigned to the Cx Program and tracks and reports the Program Plan of Actions and Milestones (POA&M) items to the CxP CIO, The CxP ITSM and appropriate Project OCSOs and ISSOs are the first points of contact between Centers and the Cx Program regarding IT Security Incident Response coordination.

### 5.8 CxP Organizational Computer Security Official (OCSO)

The CxP OCSO fulfills the "OCSO" role as identified in NPR 2810.1A. Additionally, the CxP OCSO serves as the communications link between the CxP ITSM and the CxP Project OCSO (POCSO) personnel. The CxP OCSO also assigns necessary CxP participation in the TPWG and has the authority to make protection-related decisions on behalf of the CxP for IT Security.

### 5.9 CxP Information System Security Official (ISSO)

The CxP ISSO fulfills the "ISSO" role as identified in NPR 2810.1A. Additionally, the CxP ISSO serves as the communications link between the CxP OSCO and the CxP Project ISSO (PISSO) personnel. The CxP ISSO also assigns necessary CxP participation in the TPWG and has the authority to make protection-related decisions on behalf of the CxP for IT Security.

### 5.10 Cx Projects Organizational Computer Security Official (POCSO)

Each project has a Cx POCSO who fulfills the "OCSO" defined role from NPR 2810.1A on behalf of the project to which they are assigned. The POCSO reports to the CxP OCSO primarily and communicates project level IT Security requirements to the Center ITSM.

### 5.11 Cx Projects Information System Security Officials (PISSO)

Each project designates a Cx Project ISSO to be the principal staff advisor to the information system owner on matters involving the IT security of the information system. This responsibility also include aspects of physical security, personnel security, incident handling, and security training and education relative to IT Security.

### 5.12 Center Chiefs of Security (CCS)

The CCS or Chief of Protective Services or an appropriate directorate-level official, is responsible for identifying and designating a Center TPO, COMSEC manager or specialist, Center Export Administrator (CEA), and other subject matter experts to ensure implementation and compliance with agency and local security, export control, and technology protection policies and procedures, as well as with other applicable federal regulations.

### 5.13 Center and Lead Counterintelligence Officer

The OSPP has assigned a Counterintelligence Special Agent (CISA) from each Center, which the CxP will leverage, to support the CxP. The CI community develops and provides a tailored CI Support Plan (CISP) to the PM which outlines CI responsibilities and ensures personnel are aware of the threats directed at systems and technologies. The CISA has unilateral authority to pursue CI and Counterterrorism (CT) matters to ensure full compliance with NPR 1660.1, Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirements.

### 5.14 Center Technology Protection Officer (TPO)

The Center TPO or designee is the principal Center representative to the ESMD TPWG and works closely with the ESMD TPM or designee, CxP TPO, CEA, and other government and industry security experts to ensure compliance with security, export control, information technology, and technology protection requirements at their respective Centers. The CxP leverages existing Center TPOs to fulfill these roles.

### 5.15 Center Export Administrator (CEA)

The CEA serves as the Center authority on matters related to export control and international technology transfer and is the principal Center point-of-contact with the HQ Export Administrator (HEA). The CEA is responsible for maintaining an export control program that consists of trained civil service personnel who provide guidance and export control support to the CxP and its projects. The CxP leverages existing Center CEAs to fulfill these roles.

### 5.16 NASA Contracting Officer (CO)

The CO is the NASA official with the authority to enter into, administer, and terminate contracts and make related determinations and findings. The CxP leverages existing COs fulfill these roles.

### 5.17 NASA Contracting Officer's Technical Representative (COTR)

The COTR is the person to whom the CO delegates certain contract administration responsibilities, usually related to technical direction and acceptance issues. The CxP leverages existing COTRs to fulfill these roles.

## 6.0 Security and Technology Protection

The CxP follows the security requirements identified in NPD 1600.2D, NPR 1600.1, and NPR 2810.1A. This includes provisions to protect personnel, facilities, mission-essential infrastructure, systems, and mission critical information from potential threats and other vulnerabilities that may be identified during the security risk assessment process. SMP Book 4 (CxP TPPP) identifies specific program processes and requirements regarding MEI/MCI/TVA assessments, CI, CT, and risk management/analysis.

The CxP delegates IT security program responsibilities in accordance with NPR 2810.1A and all applicable Federal regulations. This SMP and other approved CxP

plans and procedures may add additional roles and responsibilities associated with CxP IT Security.

## 6.1 IT Security

CxP IT security activities include the selection, implementation, and maintenance of security controls used to mitigate IT security risks that may affect the CxP. CxP IT security activities include IT security risk assessments that support the selection of security controls. IT security activities also include the certification and accreditation (C&A) process, in which the accuracy of CxP System IT Security Plans are certified and an approving authority accepts the IT security related risks associated with approving the operation of CxP systems. The CxP performs these IT security activities in accordance with NPR 2810.1A and all applicable Federal regulations.

### 6.1.1 Senior IT Security Management

The CxP will leverage support from the NASA CIO. The NASA CIO maintains an effective and economical information resource management (IRM) program and is ultimately responsible for IT security and has the management oversight responsibilities for ensuring the confidentiality, integrity, and availability of IT resources. Paragraph 2.2 of NPR 2810.1A describes the roles of senior IT security management with the flow of IT security policy and requirements illustrated in Figure 6.1.1-1 entitled NASA Senior IT Security Management Working Relationship.

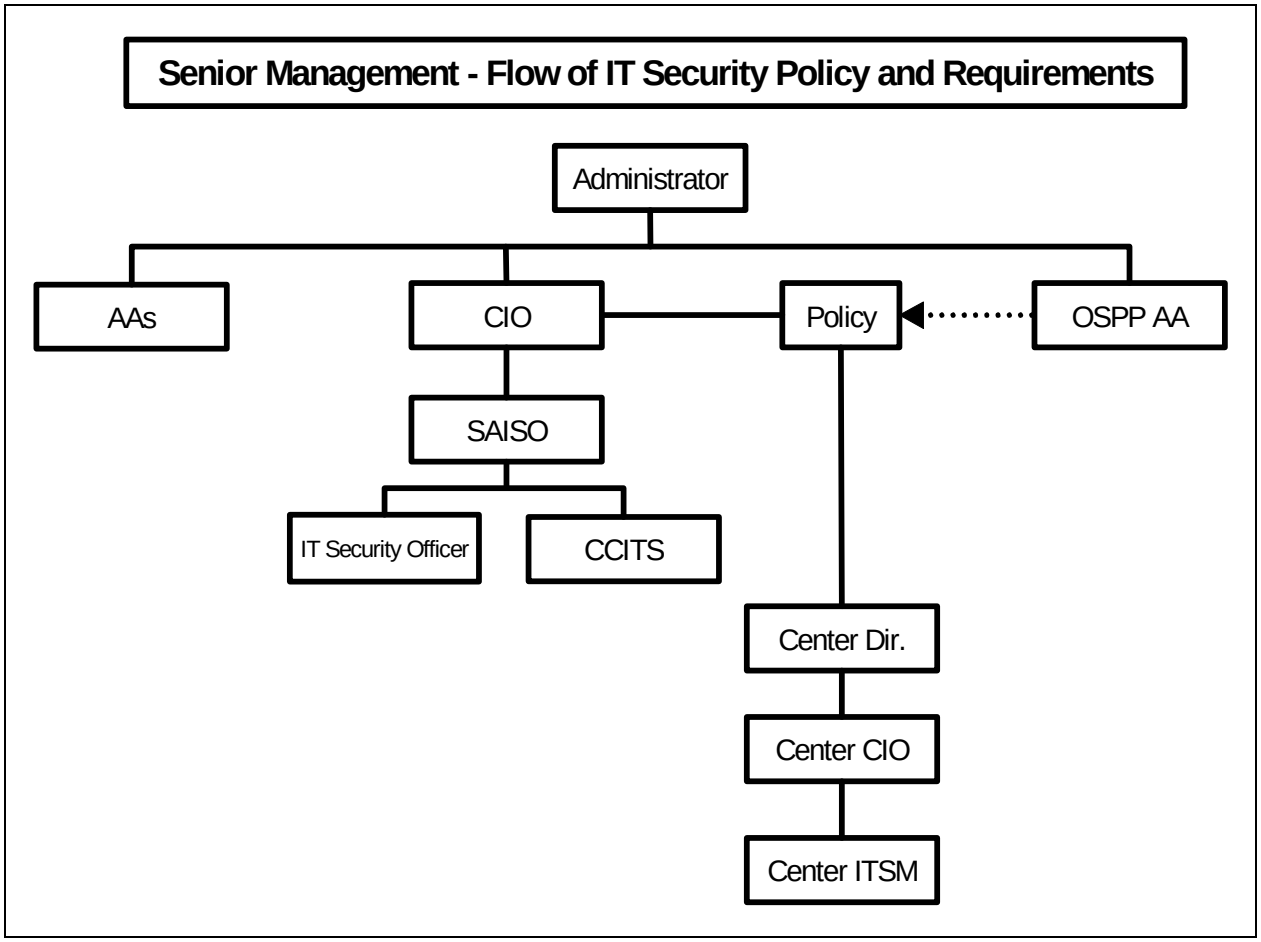


**Figure 6.1.1-1, NASA Senior IT Security Management Working Relationship**

### 6.1.2 IT Security System/Information Owners, OCSO, and ISSOs

Paragraph 2.3 and Figure 2-2 of NPR 2810.1A describe the roles of key individuals at both the Agency and Center levels for ensuring that the CxP has a sound IT security program, as well as the reporting and organizational structure. Information system owners and information owners (program, project, or functional managers) are responsible for notifying the CxP ITSM and OCSO of the existence of wholly-owned program systems, ensuring that the system development life cycle security requirements are identified during the system's initiation phase, addressed throughout design reviews, tested and verified during implementation and operational phases, and maintained during the disposition phase.

The CxP ITSM is responsible for information assurance. The CxP OCSO defines a communication process with the CxP ISSOs and Center ITSMs to ensure an effective and auditable IT security program for the CxP. The CxP IT Security Hierarchy is illustrated in Figure 6.1.2-1 entitled IT Security Organizational Flow Diagram.

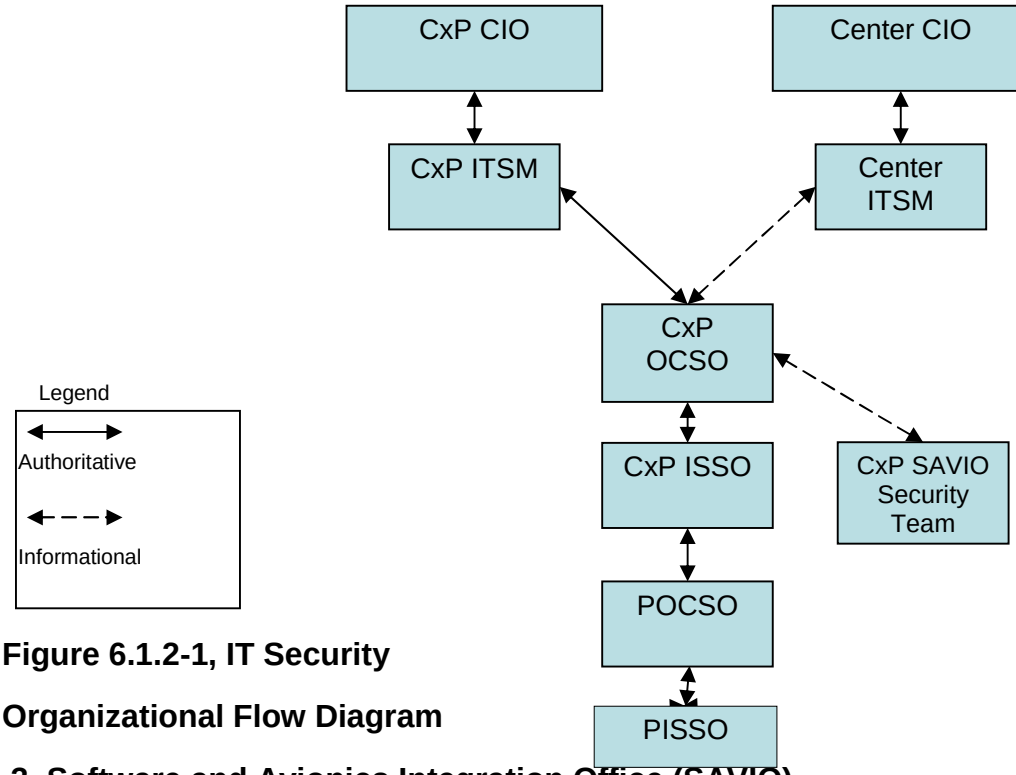


**Figure 6.1.2-1, IT Security Organizational Flow Diagram**

### 6.1.3 Software and Avionics Integration Office (SAVIO)

The Software and Avionics Integration Office (SAVIO) resides within the Systems Engineering and Integration Directorate of the Constellation Program.
SAVIO supports the IT security planning of the Constellation Program and its Projects. SAVIO further assists in the threat and vulnerability assessments, determination of security risks, and development of high-level IT security architecture.

SAVIO supports Level II requirements, architecture, test/verification processes, and modeling/simulation to ensure security is properly integrated into the designs and into the project's reviews. SAVIO supports the IT security planning of the Constellation Program and its Projects by coordinating threat and vulnerability assessments, producing a high-level IT security architecture and design requirements for the security controls which mitigate risks, and providing feedback to system owners and security officials regarding their IT System Security Plans and other documentation on IT security controls.

### 6.1.4 IT Security Threat and Vulnerability Assessment (TVA)

The CxP conducts an IT Systems' TVA using the collaborative services of an external Government agency for the Program and its Projects' IT systems that have been determined as High Impact category per FIPS 199. The IT Security TVA is done early in the IT Security Risk Assessment process and is revisited whenever a certification or re-certification is required in the C&A process -- due to changes in IT Systems architectures and/or when more up-to-date external information dictates a revisit.

The CxP and its Projects' IT systems that have been determined as moderate impact category per FIPS 199 do not need to perform the TVA, unless otherwise instructed to do so by the CxP OCSO. It can reasonably be assumed that contractor IT systems will be classified as moderate or low impact and do not need the perform the TVA, unless otherwise directed by the CxP.

The CxP and its Projects' IT systems that have been determined as low impact category per FIPS 199 do not need to perform the TVA.

The efforts, roles, responsibilities and schedules of the collaborative TVA participation are followed as defined and outlined in the IT Security TVA Process Plan {TBD}.

## 6.2 Communications Security

COMSEC involves the maintenance, operation, or control of equipment or systems used in the protection of SBU and classified data and information involved in transmitted communications or operations. The CxP, upon successful determination and implementation of IT Security Controls in response to FIPS 199/200, implements COMSEC to protect unclassified information and materials, including SBU, that are of significant importance such that if disclosed to the general public or undesirable individuals, could cause serious loss or damage to the CxP's assets, Human life or supporting IT Systems.

CxP facilities or systems are reviewed and approved by the CxP OCSO to ensure COMSEC protection measures and security controls for availability, integrity, and confidentiality are implemented in accordance to CxP IT Systems Security Plans.

The CxP follows the roles, responsibilities, procedures and guidelines as defined in NPR 1620.4, National Security Systems, Section 6 – COMSEC pertaining to the handling, control, access, categorization and use of COMSEC services and devices

to protect the data and information being communicated, when applicable. This ensures that the Cx Program follows strict and enforceable sets of processes and approaches when COMSEC services are employed during telecommunications, consistent with requirements found in NASA Policy Requirements and Standard Operating Procedures.

The CxP and its associated contractors consider all national documentation described in the policies, procedures, and instructions for the control, safeguarding and handling of COMSEC equipment and materials. All NASA and Contractor personnel with responsibilities related to the Cx Program understand the importance of the information and materials under their control.

### 6.2.1 Applicability

The CxP Projects adopt those roles and responsibilities from the various sections of NPR 1620.4 as outlined in Table 6.2.1-1 - Applicability Matrix for COMSEC Guidelines.

**Table 6.2.1-1, Applicability Matrix for COMSEC Guidelines**

| NPR 1620.4 Section(s) | CxP | GOP | MOP | Ares (I&V) | LSS | Orion | Altair | EVA |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Section 6.1 | √ | √ | √ | √ | √ | √ | √ | √ |
| Section 6.2 | √ | √ | √ | √ | √ | √ | √ | √ |
| Section 6.3 | | | | | | | | |
| Section 6. 4 | √ | √ | √ | TBR | √ | √ | √ | |
| Section 6.5 | √ | √ | √ | PBT | √ | √ | √ | √ |
| Section 6.6 | √ | √ | √ | | | | | |

## 6.3 Export Control Compliance

In the interest of national security and foreign policy considerations, the export of all products, technical data, and services in support of the Government is controlled by various U.S. laws and regulations. Compliance with export laws and regulations, whether in the U.S. or abroad, is required by all CxP personnel.

In addition to the International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and other applicable U.S. export regulations, controls of both data and hardware exports by Cx Program and Project personnel are implemented in accordance with NPR 2190.1, NASA Export Control Program, NPR 2200.2B, Requirements for Documentation, Approval, and Dissemination of Scientific and Technical Information, and unique Center work instructions or directives. Export requirements apply to all activities and products produced or received and funded through the Cx P. These products are required to accomplish program and project objectives, which may involve the transmittal of hardware, software, or technical information to destinations outside the U.S. or to foreign persons within the U.S.

Detailed requirements to ensure export control compliance are in Center-specific plans and procedures or each project level export control plan.

## 6.4 Physical and MEI Security

A physical security program is required at all CxP facilities to protect personnel and assets. Existing Center or site-specific physical security plans and procedures used by the CxP are assessed for continuity with this SMP, NPR 1600.1, and NPR 1620.3, Physical Security Requirements for NASA Facilities and Property. The CxP leverages support from each CCS to implement a proactive physical security program that includes, as a minimum, building checks, tracking systems for lost and stolen property, lock and key control and inventory program, electronic security systems controls, investigations of lost and stolen property, and loss prevention surveys and reporting in accordance with NPR 1600.1.

The CxP maintains a consolidated list of all CxP MEI assets. The CxP and contractors establish and maintain procedures to meet physical and/or MEI security requirements as outlined in Table 6.4-1.

**Table 6.4-1, Applicability Matrix for Physical/MEI Security**

| **Physical/MEI Security** | NPR 1600.1 | NPR 1600-1 | NPR 1620.2 & 1620.3 | NPR 1040.1 & 8715.2 | NPR 1371.2A | NPR 1660.1 | NPR 2810.1A | HSPD 7 & 12 | 14 CFR, Part 1205 Subpart 10 | SMP Book 3 |
|---|---|---|---|---|---|---|---|---|---|---|
| NASA Critical Infrastructure & Key Resources - MEIPP | √ | | | √ | | √ | | | | √ |
| Badging & Access Controls | √ | √ | | √ | | | | | | √ |
| Security Control Centers | | | | √ | | | | | | √ |
| Access to Offsite Facilities | √ | √ | | | | | | √ | | |
| **Physical/MEI Security** | NPR 1600.1 | NPR 1600-1 | NPR 1620.2 & 1620.3 | NPR 1040.1 & 8715.2 | NPR 1371.2A | NPR 1660.1 | NPR 2810.1A | HSPD 7 & 12 | 14 CFR, Part 1205 Subpart 10 | SMP Book 3 |
| Access to NASA Installations | √ | | | √ | | | | | | √ |
| Visits by Foreign Nationals/Reps | √ | | | | √ | √ | | | | |
| Weapons Control | √ | | | | | | | | | |
| Employee Terminations and Transfers | √ | | | | | | √ | | | |
| Investigations | √ | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Vehicle Integrity: Perimeter Area Protection & Control | √ | | √ | | | | | | √ | |
| Onsite/Offsite Secure Areas & Inspections | √ | | √ | √ | | | | | √ | |

### 6.4.1 Vehicle Integrity

The CxP ensures that NASA and contractor security personnel monitor and control access to the Crew Exploration Vehicle (CEV), Crew Launch Vehicle (CLV), and Cargo Launch Vehicle (CaLV). Controls should include, but are not limited to, requirements for ingress and egress from the CEV, CLV, CaLV, launch system stages, and associated processing areas.

### 6.4.2 Transport Security

#### *6.4.2.1 Protection in Transit*

The CxP ensures that protection of flight hardware or components in test facilities, in transit to final assembly, and at launch facilities is consistent with appropriate security requirements and risk management strategies.

#### *6.4.2.2 Protection in Recovery*

The CxP ensures that protection of flight hardware or components recovered for re-use (e.g., rocket boosters) or post-mission (e.g., crew module) is in accordance with CxP selected safeguards.

#### *6.4.2.3 Protection in Storage*

Protection of flight hardware or components in storage is consistent with CxP selected safeguards and site security provisions. Specifically, access to NASA and Government installations, or into controlled areas within NASA and Government installations and security areas (limited or closed) on NASA installations, require prior authorization. Use of an area permit system supplements NASA-issued identification badges. When special operational safety or other conditions are in effect, special

badges, access lists, or other devices authorized by the CCS may be used to grant access.

### 6.4.3 Critical Incident Reporting and Investigations

In accordance with paragraph 1.3.8. of NPR 1660.1, "NASA employees, contractors, and other individuals associated with NASA are required to appropriately protect classified and sensitive information. Accordingly, individuals associated with NASA are obligated to report incidents to a NASA CISA when they suspect that sensitive and/or classified information may be at jeopardy and subject to compromise. All such individuals are required to report unusual or suspicious overtures by a foreign national or a representative of a foreign entity, whether or not sensitive and/or classified information is believed to be in jeopardy."

Notification of all ongoing investigations involving CxP activities are submitted through the CxP TPO or OCSO to the TPWG for further reporting to HQ OSPP and HQ DIO, as appropriate. Information that is considered sensitive to the investigation may be omitted in the initial reporting.

CxP team members have a responsibility for immediately reporting incidents that may negatively impact NASA and the CxP. At a minimum, the following incidents are reported immediately to the CCS, Center TPO, CxP TPO, CxP OCSO, Project TPO, Project OCSO, and ISSO:

- Evidence or suspicion of penetration of a security area or IT network
- Suspicion of deliberate damage to assets
- Equipment malfunctions of a suspicious or unusual nature
- Damage to critical hardware
- Loss or compromise of sensitive or classified information

## 6.5 Industrial/ Information Security

This section describes the protective measures required for protecting classified and unclassified sensitive information. As applicable, the respective CxP contractors operate in compliance with requirements set forth in the DoD NISPOM, NPR 1600.1 (Chapters 2, 5, and 6), NASA Site-Specific Regulations, DD Form 254, and all other contractually-specified requirements.

### 6.5.1 DoD National Industrial Security Program Operating Manual (NISPOM) and NASA Requlations

The forms commonly used as checklists for security and technology protection are DD Form 254, Contract Security Classification Specification, NASA Form 1733, Information and Technology Classification and/or Sensitivity Level Determination Checklist, and NASA Form 1686, Sensitive But Unclassified Information.

#### *6.5.1.1 DoD NISPOM and DD Form 254 (Industrial Security)*

CxP contracts that require access to classified information or areas are processed in accordance with Chapter 6 of NPR 1600.1, DoD 5220.22M (NISPOM), and the DD Form 254. These requirements, restrictions, and safeguards are necessary to prevent unauthorized disclosure of classified information and to control the unauthorized disclosure of NASA-released classified information. Unsatisfactory contractor security conditions are reported to the cognizant Defense Security Services (DSS) office, CCS, TPWG, Center TPO, and Cx Project or Program TPOs.

#### *6.5.1.2 NASA Form 1733 – Information and Technology Classification and Sensitivity Level Checklist (Information Security Management)*

NASA Form 1733, Information and Technology Classification and/or Sensitivity Level Determination Checklist, completed by the NASA PM, is a permanent program document in accordance with paragraph 5.23 of NPR 1600.1. Upon identification of sensitive information or technologies, the program or project element and external partners work together to ensure the overall protection of NASA MCI, MEI assets, classified national security information (CNSI), and SBU information. After sensitive information or technologies have been identified in association with a program or project, contractor organizations are required to participate in the overall TPP process as appropriate for their scope of effort in accordance with the SMP Book 4 (TPPP).

#### *6.5.1.3 NASA Form 1686 – SBU Information (Information Security Management)*

SBU policy requirements and guidelines are defined in Chapter 5.24 of NPR 1600.1. The detailed processes on how to correctly identify, designate, mark, protect and decontrol SBU are described in an ESMD SBU Work Instruction which can be found on the CxP ICE (Integrated Collaborative Environment) homepage.

Section 1.3 of the ESMD-SBUWI1 describes the specific responsibilities and authority of the designating officials, originators, custodians, and holders when reviewing information as SBU. The work instruction also describes the detailed

protection measures required for telephone conversations, mailing, electronic transmission and storage including e-mailing, faxing and virtual meetings, physical storage, and how to conduct meetings and collaboration containing SBU information. Paragraph 5.24.3 of NPR 1600.1, describes transmission, storage, and destruction of SBU information.

All CxP employees comply with Chapter 5.24 of NPR 1600.1 and the ESMD SBU Work Instruction for handling SBU information. Assistance in determining appropriate document markings, safeguarding, and destruction may be obtained through the CCS, CEA, or Center and Cx Program or Project TPOs. Personnel can be subject to administrative sanctions if they fail to protect or properly handle SBU information.

### 6.5.2 Security Violations

Security incidents involving any loss or suspected compromise of classified information or material are reported immediately to the CxP TPO, CCS, and cognizant DSS. Any loss or compromise of SBU or MCI (including export control) is reported to the CxP TPO who ensures that the TPWG and Center TPOs are knowledgeable of all security violations. The CxP ensures a corrective action plan is developed to prevent a recurrence.

Specific details that may compromise the investigation may be omitted in the report but must be made available to the authorized personnel with proper clearances.

## 6.6 Personnel Security

Background investigations are processed and adjudicated by NASA personnel security specialists before access to NASA facilities, IT resources, and CNSI can be granted.

#### 6.6.1 Certification and Investigation Process for IT and MEI

Background investigations are required for all CxP personnel who require access to IT and MEI resources and facilities in accordance with NPR 1600.1 (Chapters 3 and 4), HSPD 7, Critical Infrastructure Identification Prioritization and Protection, HSPD 12, Personal Identity Verification/Validation, and Center-specific policies and procedures. The U.S. Office of Personnel Management (OPM) Condensed Agency Users Manual for Electronic Questionnaires for Investigations Processing System (Version 2.00.02, June 2006) is used by NASA security personnel to submit requests for background investigations.

### 6.6.2 Foreign Nationals

All foreign nationals who are currently in the U.S. and who require background investigations as set forth in NPR 1371.2A, Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Representatives of Foreign Entities (with Change 1), are subjected to a national agency check with inquiries (NACI). Effective November 9, 2006, foreign nationals having national agency checks (NAC), which have been completed within the past five years, are not required to be reinvestigated with an NACI; however, upon renewal of their background investigations, a NACI is required. The OPM and CCS require that foreign nationals who do not have social security numbers (SSN) have their NACI information submitted via the paper forms, along with fingerprint cards.

### 6.6.3 Adverse Information

When adverse information is developed or received in the course of any personnel security investigation or subsequent to such investigation and initial favorable determination made, the scope of inquiry normally is expanded to the extent necessary to obtain sufficient information to make a sound determination regarding access granted. All CxP employees who are approved for access to classified information or NASA IT and MEI programs are required to report any adverse information immediately to their management. NASA managers, contractor managers, and security officers are required to provide adverse information reports immediately to the CCS. Specific guidance is provided in NPR 1600.1, Chapter 3 for NASA personnel, and Chapter 4 for contractor personnel.

## 6.7 Contractor Security

Contractor facility security officers (FSO) or managers have a direct internal customer relationship with the respective company senior management at all operating locations. In addition, Center-specific technology protection, export control, and security policies and procedures, as well as the DoD and DSS regulations for classified operations (if applicable), apply to each location.

The contractor operates as an integrated organization responding to priorities and functional criticalities and changing resource demands. Interface with NASA officials and with each subcontractor occurs as needed to provide program-wide focus and maintenance of operations.

The contractors immediately notify the CO and COTR of any unsatisfactory security conditions in the contractor or subcontractor's facility. Any new security or technology protection tasks or related tasks not identified in the SOW are approved by the CO or COTR or both before implementation.

The CxP TPO and OCSO, with support from the CCS and TPWG, are responsible for auditing, inspecting, or monitoring CxP contractor security programs to ensure compliance with this SMP, associated books, and their statement of work (SOW). Various methods may be used (e.g., quarterly meetings, metrics reports, etc.). For example, the audit may consist of a one-day surveillance visit to assess how the contractor's internal security policies meet the intent of security requirements identified in the IT Security Plan. All security and technology protection requirements identified in Section 6.0 are included in the COTR's performance evaluation of all contractors and their subcontractors.

# 7.0 Security Awareness and Training

CxP employee security awareness is achieved through communication and training to ensure security responsibilities are understood and practiced. This is accomplished by each performing organization, through the implementation of a Basic Security Awareness and Training Program, which includes the NASA or contractor designed computer-based training (CBT) or formal briefings arranged by each CxP contractor security officials. Additional security awareness multimedia may involve the use of video, graphics (handouts, posters), audio etc.

TPWG members, Center security, export control, IT security, and technology protection personnel ensure that content relevant security awareness briefings and training are provided for CxP personnel in the following areas as a minimum:

- Technology protection
- IT security
- Export control
- Physical and personnel security
- Industrial and information security
- COMSEC
- CI awareness

Physical and personnel security awareness briefings and training are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance, including NPR 1600.1, NPR 1620.2, and the DoD NISPOM.

All CxP employees receive appropriate security awareness training as part of their employee orientation. Annual NASA refresher training on a variety of security subjects is provided through the NASA learning management system, System for Administration, Training, and Educational Resources for NASA (SATERN). SATERN modules may be provided to contractor organizations as needed.

## 7.1 Industrial, Information, and COMSEC Security Training

The NISPOM identifies and delineates the requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information and SBU and to control the authorized disclosure of information released.

CxP COMSEC personnel are certified in COMSEC procedures as applicable for their task assignments in accordance with NPR 1620.4.

## 7.2 Information Technology Security Training

IT security awareness or training is completed in accordance with NPR 2810.1A, Chapters 14 and 18. All NASA employees and contractors must complete the SATERN IT Security Awareness Training modules annually or other Agency approved training.

# 8.0 Reporting

The reporting of metrics will assist the CxP management in assessing the effectiveness of security measures and countermeasures implemented to block or mitigate vulnerabilities.

## 8.1 Metrics and Reporting

Metrics are defined to provide insight to CxP management into the effectiveness, progress, and value added aspects of the CxP TPP. CxP metrics identified in this section are intended to measure the effectiveness of the Cx Security Program and are derived from the tasks and products described in CxP 70170 (Functional Security Requirements), CxP 70171 (Information Technology Security Architecture), SMP Book 3 (Disaster Recovery, Continuity of Operations, and Emergency Response Plan), and SMP Book 4 (TPPP).

The CxP TPO provides security metrics to the Cx PM on a monthly basis, unless directed otherwise in writing. At a minimum, metrics include the following:

- Critical incident reports, security violations, adverse information reports, investigations
- Progress on security, technology protection, export control, and IT security countermeasures deployments
- Status of CxP MEI assets
- Status of CxP MCI assessments
- Risk analysis on both industrial and IT security processes
- Security education and awareness training

The goal of this section is to meet any reporting requirements whether levied by the Cx Program, Agency, or Office of Management and Budget.

## 8.2 Audits and Reviews

The TPWG and Center security, export control, and technology protection personnel conduct program and project staff assistance visits to review and audit the effectiveness of the TPP on an annual basis to ensure policy compliance regarding the security disciplines identified in this plan.

### 8.2.1 Audits

CxP systems or organizations develop, disseminate, and periodically review and update the following:

- A formal documented audit and accountability policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance
- Formal documented procedures to facilitate the implementation of the CxP audit and accountability policy and associated CxP audit and accountability controls

Advance notification of audits is provided to the CxP and Project Managers. The CxP TPO, OCSO, and Project Managers ensure that semi-annual self-inspections are conducted and documented in accordance with established procedures or directives. The TPWG advises and supports the PM with ongoing monitoring of MCI and the effectiveness of their protection measures.

### 8.2.2 Quarterly Reviews

TPWG members (NASA and contractors) participate in quarterly reviews and bi-weekly teleconferences by providing presentations or status updates of security activities associated with their project. At a minimum, the quarterly reviews include the following:

- Metrics, which include critical incident reports, security violations, adverse information reports, investigations, cost effectiveness of operations
- Progress reports in system security, physical/MEI security, technology protection, counterintelligence security, export control, IT security, and information assurance
- Risk management process
- Security education and awareness
- Training

### 8.2.3 Vulnerability Scans

Vulnerability scanning is required by the Cx P at least quarterly and upon request of the CxP ITSM or CxP OCSO. The CxP will rely on Center and contractor infrastructures to perform vulnerability scanning and reporting activities as established at those facilities. The process for notification, conducting, and reporting scan results is governed by the CxP IT security organization and is consistent with a memorandum of agreement (MOA) for CxP IT security scans as established with each of the appropriate NASA Centers.

Vulnerability scanning is conducted by CxP IT security representatives and is intended to identify potential weaknesses in IT facilities and systems. CxP facilities and systems are scanned at least quarterly or upon request. All vulnerability scanning is conducted by using industry-standard commercial off-the-shelf (COTS) automated scanning software.

### 8.2.4 Incident Handling and Investigation

In addition to complying with the Agency standard incident handling processes, security incidents (e.g., breaches of established IT or physical security, including potential incident occurrences) are reported to the CxP TPO and OCSO, until dispositioned to closure for all CxP facilities and systems.

## A1.0 Acronyms and Abbreviations

| | |
| --- | --- |
| AA | Associate Administrator |
| CARD | CxP [Constellation Program] Architecture Requirements Document] |
| CaLV | Cargo Launch Vehicle |
| CCI | Controlled Communications Security (COMSEC) Items |
| CCITS | Competency Center for IT Security |
| CCS | Center Chief of Security |
| CEA | Center Export Administrator |
| CEV | Crew Exploration Vehicle |
| CFR | Code of Federal Regulations |
| CI | Counterintelligence |
| CIO | Chief Information Officer |
| CISA | Counterintelligence Special Agent |
| CISP | CI Support Plan |
| CLV | Crew Launch Vehicle |
| CNSI | Classified National Security Information |
| CO | Contracting Officer |
| COMSEC | Communications Security |
| COOP | Continuity of Operations Planning |
| CoP | Community of Practice |
| COR | Center Office of Records |
| COTR | Contracting Officer's Technical Representative |
| COTS | Commercial off-the-Shelf |
| CR | Change Request |
| CRM | Continuous Risk Management |
| CSOP | COMSEC Standard Operating Procedures |
| CT | Counterterrorism |
| Cx | Constellation |
| Cx CB | Constellation Control Board |
| CxP | Constellation Program |
| DES | Data Encryption Standard |
| DIO | Directorate Integration Office |

| | |
| --- | --- |
| DoD | Department of Defense |
| DSS | Defense Security Services |
| DUI | Driving Under the Influence |
| EAR | Export Administration Regulations |
| ESMD | Exploration Systems Mission Directorate |
| EVA | ExtraVehicular Activity |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FSO | Facility Security Officer |
| HEA | Headquarters [HQ] Export Administrator |
| HQ | Headquarters |
| HSPD | Homeland Security Presidential Directive |
| IA | Information Assurance |
| ICE | Integrated Collaborative Environment |
| IRM | Information Resource Management |
| ISSO | Information System Security Official |
| ISSP | International Space Station Program |
| IT | Information Technology |
| ITAR | International Traffic in Arms Regulations |
| ITSM | Information Technology Security Manager |

| | |
| --- | --- |
| MCI | Mission Critical Information |
| MEI | Mission Essential Infrastructure |
| MEIPP | Mission Essential Infrastructure Protection Program |
| MOA | Memorandum of Agreement |
| MSFC | Marshall Space Flight Center |
| NAC | National Agency Check |
| NACI | National Agency Check with Inquiries |
| NASA | National Aeronautics and Space Administration |
| NISPOM | National Industrial Security Program Operating Manual |
| NIST | National Institute of Standards and Technology |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |
| OCA | Original Classification Authority |
| OCIO | Office of Chief Information Officer |
| OCSO | Organizational Computer Security Official |
| OIG | Office of Inspector General |
| OPM | Office of Personnel Management |
| OPR | Office of Primary Responsibility |
| OSPP | Office of Security and Program Protection |
| PISSO | Projects Information System Security Officials) |
| PM | Program Manager |
| PMP | Program Management Plan |
| POA&M | Program Plan of Actions and Milestones |
| POCSO | Project Organizational Computer Security Official |
| PP&C | Program, Planning and Control |
| PS | Protective Services |
| RAA | Risk Acceptance Authority |

| | |
| --- | --- |
| SAISO | Senior Agency Information Security Officer |
| SATERN | System for Administration, Training, and Educational Resources for NASA |
| SAVIO | Software and Avionics Integration Office |
| SBIR | Small Business Innovative Research |
| SBU | Sensitive But Unclassified |
| SMP | Security Management Plan |
| SOMD | Space Operations Mission Directorate |
| SOP | Standard Operating Procedures |
| SOW | Statement of Work |
| SP | Special Publication |
| SSE | System Security Engineering |
| SSN | Social Security Number |
| SSP | Space Shuttle Program |
| STI | Scientific and Technical Information |
| TBD | To Be Determined |
| TBR | To Be Resolved |
| TPM | Technology Protection Manager |
| TPO | Technology Protection Officer |
| TPP | Technology Protection Program |
| TPPP | Technology Protection Program Plan |
| TPWG | Technology Protection Working Group |
| TVA | Threat and Vulnerability Assessment |
| U.S. | United States |
| WBS | Work Breakdown Structure |

## A2.0 Glossary of Terms

**Acquisition.** The acquiring, by contract, of supplies or services (including construction) through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, or evaluated. Acquisition begins at the point when Agency needs are established and includes the description of requirements to satisfy Agency needs, solicitation, and selection of sources, award of contracts, contract financing, performance, administration, technical, and management functions directly related to the process of fulfilling Agency needs by contract.

**CI Threat and Vulnerability Assessment.** A formal, in-depth review and evaluation of the capabilities and interests of identified aggressors for the purpose of determining their potential for targeting NASA operations and assets.

**Communications Security (COMSEC)** - The protection resulting from the application of crypto security, transmission security, and emission security measures to telecommunications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value that might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

**Configuration Management**. A management discipline applied over the product's life cycle to provide visibility and to control performance and functional and physical characteristics.

**Constellation Program Control Board.** A panel structured for making decisions that affect the baseline, as well as for making technical implementation decisions at a program level. An example of the decisions that affect the baseline would be anything that requires a change to a Program approved document. An example of a technical implementation decision would be whether to approve a design modification requiring additional funding. The Board is chaired by the Program Manager and membership includes each project and program appearing in Figure 1.5-1 of this SMP, as well as technical authorities. This panel represents the interests of program and project management by ensuring that a structured process is used to consider proposed changes and incorporate them into a specified release of a product. The Board requests that impact analysis of proposed changes be performed, reviews change requests, make decisions, and communicate decisions made to affected groups and individuals.

**Contingency.** Reserves, including funding, schedule, performance, manpower, and services, allocated to and managed by the Program/Project Manager for the resolution of problems normally encountered to mitigate risks while ensuring compliance to the specified program/project scope.

**Counterintelligence.** Information gathered and activities conducted to protect against espionage, sabotage, and other intelligence activities conducted for or on behalf of foreign powers, organizations or persons, or international and domestic terrorist activities. Counterintelligence functions are distinct from, but work cooperatively with, Agency security disciplines.

**Counterterrorism.** A NASA CI activity to protect NASA assets from terrorist activities, both foreign and domestic.

**ESMD Technology Protection Community of Practice Website.** A secure communication tool on which multi-disciplined stakeholders discuss, status, and resolve issues and concerns relative to security and technology protection.

**Foreign National.** For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States. Includes lawful permanent resident (e.g., holders of green cards) or persons admitted with refugee status to the United States.

**Foreign Person.** Any person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). Also means any foreign corporation, business association, partnerships, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

**Foreign Representative.** Any person, including a U.S. citizen or permanent resident alien or protected individual, representing a foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments.

**Implementation**. The execution of approved plans for the development and operation of programs and projects, the establishment of control systems to ensure performance to plan, and alignment with current Agency strategies.

**Information Technology (IT)**. Hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other.

**IT Security TVA**. CxP-unique process which seeks external collaborative information in support of the Risk Assessment (RA) process described in NIST SP 800-30 and conducted on CxP IT Systems. The process captures inputs from external subject matter experts/organizations relative to validated threats and vulnerabilities, provides NASA a more comprehensive and accurate assessment of the security risks against CxP IT Systems, and allows for an informed basis on which to select/modify security controls.

**Level I.** Directorate level authority.

**Level II.** Program level authority.

**Level III.** Project level authority.

**Level IV.** Elements (contractors, subcontractors, etc.).

**Metric.** A measurement taken over a period of time that communicates vital information about a process or activity. A metric should drive appropriate action.

**Mission Critical Information.** Information for which NASA is responsible that is related to research, technologies, projects, programs, or systems that, if released outside established protocols, would:

(1) Significantly affect NASA resources, requiring additional research, development, tests, or evaluation to overcome the adverse affects of unauthorized release; or,
(2) Significantly reduce the performance or effectiveness of NASA research, projects, technologies, programs, or systems; or,
(3) Negatively alter the direction of NASA research, projects, technologies, programs, or systems, thus reducing NASA's and the nation's advantage in space technologies

**Mission Essential Infrastructure.** Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations. These resources may include critical components and facilities associated with the Space Shuttle, expendable launch vehicles, associated upper stages, Spacelab, International Space Station, command communication and control capability, Government-owned flight or experimental flight vehicles and apparatus, and one-of-a-kind irreplaceable facilities.

**Mission Essential Infrastructure Protection Program.** The planning and implementation, of an enhanced protection level for Agency key resources identified by an NASA organization to be so crucial to the success of NASA missions as to warrant protection over that which would be routinely provided to NASA assets.

**National Security Positions** - Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

(1) ***Confidential*** - Information, the unauthorized disclosure of which reasonably could be expected to cause damage to National security that the Original Classification Authority (OCA) is able to identify or describe.

(2) ***Secret*** - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to National security that the OCA is able to identify or describe.

(3) ***Top Secret*** - Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National security that the OCA is able to identify or describe.

**Program**. A strategic investment by a Mission Directorate or Mission Support Office that has a defined architecture, requirements, funding level, and a management structure that supports one or more projects.

**Project.** A specific investment identified in a Program Plan having defined requirements, a life-cycle cost, a beginning, and an end.

**Risk.** The combination of the probability that a program or project will experience an undesired event (some examples include a cost overrun, schedule slippage, safety mishap, health problem, malicious activities, environmental impact, failure to achieve a needed scientific or technological breakthrough or mission success criteria) and the consequences, impact, or severity of the undesired event, were it to occur. Both the probability and consequences may have associated uncertainties.

**Risk Assessment.** A formal process whereby a project, program, or event is evaluated to determine the types and level of risk associated with its implementation. An evaluation of a risk item that determines (1) what can go wrong, (2) how likely is it to occur, and (3) what the consequences are.

**Risk Management**. An organized, systematic decision making process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk to increase the likelihood of achieving program/project goals. A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

**Risk Acceptance.** An official acknowledgement by a management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate the risk.

**Risk Acceptance Authority.** An individual designated in writing who makes the final determination on waivers to security standards and requirements when a security deficiency has been determined to pose a serious risk to a program.

**Safety.** Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

**Security**. Protection of people, property, and information assets owned by NASA which covers physical assets, personnel, IT, communications, and operations.

**Security Violation.** An act or action by an individual or individual(s) that is in conflict with NASA security policy or procedure (e.g., loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; security area violations, etc.).

NOTE: Does not include incidents of criminal activity (e.g., theft, assault, DUI, etc.)

**Sensitive But Unclassified (SBU) Information.** In accordance with NPR 1600.1, it is information, regardless of its form (visual, oral, or recorded such as digital, hard-copy, magnetic tape, etc.), the release of which could cause harm to a person's privacy or welfare, that adversely impact economic or industrial institutions, or compromise programs or operations essential to safeguarding our national interests may be designated as SBU under NASA's SBU policy requirements and guidelines. Common examples of SBU information include export-controlled data (designated as SBU on a discretionary basis) under the ITAR or EAR, proprietary information including trade secrets and commercial or confidential financial information, source selection and proposal information, small business innovative research (SBIR) data, privacy act information including personnel records and medical information, national space policy not yet publicly released, drawings and specifications of specific MEI information and others.

**System.** Physical entities that have functional capabilities allocated to them necessary to satisfy Architecture-level mission objectives. Systems can perform all allocated functions within a mission phase, or through mated operations with other Constellation systems (e.g. Crew Exploration Vehicle, Lunar Surface Access Module).

**Systems Engineering**. A disciplined approach for the definition, implementation, integration and operation of a system (product or service). The emphasis is on achieving stakeholder functional, physical and operational performance requirements in the intended use environments over its planned life within cost and schedule constraints. Systems engineering includes the engineering processes and technical

management processes that consider the interface relationships across all elements of the system, other systems or as a part of a larger system.

**System Security Engineering.** A process established to identify and incorporate security provisions as early as possible in program or project system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

**Technology Protection.** NASA policy to establish and maintain a Technology Protection Program for the early identification and protection of Mission Critical Information (MCI) inherent in research and development, technology development, technology maturation, technology deployment and mission operations. Critical research and program technologies, systems, and information must be documented and protected to prevent unauthorized disclosures that could significantly impact cost, schedule, performance, and supportability; program direction; or lead to technology transfer outside of established protocols; or require additional resources to develop alternative technologies.

**Waiver.** The approved continuance of a condition authorized by the AA/OSPP that varies from a requirement and implements risk management on the designated vulnerability.