NASA programs and projects managed under the guidance in NPR 7120.5 and NPR 7120.8 (for research and technology projects operating in space) are required to develop a Project Protection Plan (PPP). This template is provided by the NASA Mission Resilience and Protection Program (MRPP) as a starting point to meet this requirement.

The PPP is owned by the project (or implementing organization), and usually developed under the direction of the overall project systems engineer. Most Centers have a space or mission protection team, such as GSFC’s Space Asset Protection Program (Code 599), HEOMD’s System Protection Office (SPO), or JPL’s Mission Protection group. The space or mission protection team typically provides support to the project in assisting the development of the protection plan and in reviewing the document. In addition, the space or mission protection team usually provides the primary support for classified content such as threat information.

In multiple sections, the template includes guidance text to clarify and guide the project-developed content for that section. Some of these elements may duplicate content found in other project documents. The intent of including these elements is to ensure sufficient context for the protection analysis without requiring many additional documents be at hand.

Appendix C, covering Threats, Vulnerabilities, and Risks, is not included in this template. That appendix involves Classified National Security Information (CNSI) to discuss specific threats, vulnerabilities, and associated risks. Where possible, a general risk (missing any sensitive specifics) is captured in Section 7 of this document, and is tracked in the project’s risk management system.

As long as the information and topics covered in this template are included, organizations may adapt the template as needed to follow local document structure and needs.

The minimum signatures on the PPP include the project manager, the delegated Engineering Technical Authority for Protection (usually at the Center level, sometimes at the Mission Directorate level), and the sponsoring Mission Directorate’s designee (usually Deputy AA for Programs or equivalent).

*This page should not be included in the final product.*

**Template Changelog**

|  |  |
| --- | --- |
| **Date** | **Summary of Changes** |
| 2020-12-16 | * Updated policy references
* Updated to reflect changes from STD-1006 w/change 1
* Updated to reflect changes from CPS revision 4.5
 |
| 2020-03-19 | * Initial release of MRPP template, replaces prior SAPP templates.
 |

**Project Name**

PPP Template without project content is UNCLASSIFIED

PPP template with SBU project content is SENSITIVE BUT UNCLASSIFIED.

Remove this notice and add SBU cover sheet.

**Project Protection Plan**

**XXX-MGMT-PLAN-00YY**

**Revision — Date**

****

**XYZ Center**

**City, State**

National Aeronautics and

Space Administration

**CM FOREWORD**

This document is a Project-controlled document. Changes to this document require prior approval of the applicable Configuration Control Board Chairperson or designee. Proposed changes shall be submitted to the Project Mission Configuration Management Office, along with supportive material justifying the proposed change.

In this document, a requirement is identified by “shall,” a good practice by “should,” permission by “may” or “can,” expectation by “will,” and descriptive material by “is.”

Questions or comments concerning this document should be addressed to:

Project Configuration Management Office

Mail Stop xxx

XYZ Center

City, State, Zip Code

**XXX Project Protection Plan**

**Review/Signature/Approval Page**

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

Name Date

Mission Systems Engineer

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

Name Date

Project Manager

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

Name Date

Lead, XYZ Center Space/Mission Protection Team

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

Name Date

XYZ Center

Protection Technical Authority

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

Name Date

Deputy Associate Administrator for Programs

XXX Mission Directorate

**DOCUMENT CHANGE RECORD**

Sheet 1 of 1

|  |  |  |  |
| --- | --- | --- | --- |
| REVLEVEL | DESCRIPTION OF CHANGES | APPROVED BY | DATEAPPROVED |
| - | Draft Release date |  |  |

**TABLE OF CONTENTS**

1 INTRODUCTION 6

1.1 Protection Plan Overview 6

1.2 Governance 6

1.3 References 6

2 executive summary 7

3 PROTECTION PROCESS OVERVIEW 7

4 XXX mission overview 8

4.1 XXX Program/Project Overview 8

4.2 XXX Mission Overview 8

4.3 Critical Project Technology (CPT) / Critical Project Information (CPI) 8

5 mission support elements 8

6 system criticality and susceptibilities 8

6.1 Requirements 8

6.2 Architecture 9

6.3 CONOPS 9

7 mission RISKS 10

8 protection strategies 11

8.1 Space System Protection Standard (NASA-STD-1006) Implementation 11

8.2 Candidate Protection Strategies (CPS) Implementation 12

9 Abbreviations and acronyms 15

Appendix A – NASA-STD-1006 Implementation Table for XXX 17

Appendix B – CPS Implementation Table for XXX 19

Appendix C – Threats, Vulnerabilities and Risks for XXX

# INTRODUCTION

## Protection Plan Overview

(U) The purpose of the XXX Project Protection Plan (PPP) is to address the XXX project protection strategy as required by NPR 7120.5 or NPR 7120.8 in the context of the NASA Space System Protection Standard (NASA-STD-1006) and the Candidate Protection Strategies (CPS) established by the NASA Mission Resilience and Protection Program (MRPP), and to assess threats, vulnerabilities and risks applicable to XXX. This document will be updated as necessary as further protection strategies are identified and matured over the mission lifecycle as well as project documentation availability.

(U) The scope of the XXX PPP is an assessment of the implementation of NASA-STD-1006 and the list of CPS provided by NASA MRPP, a comprehensive assessment of threats, vulnerabilities and risks applicable to XXX, and an identification of appropriate countermeasures.

## Governance

(U) The PPP was developed by the XXX project office with assistance from the XYZ Center Space/Mission Protection Team. Configuration management for the Sensitive But Unclassified (SBU) portion of the XXX PPP will be performed by the XXX configuration control board. Classified appendices will be configuration managed by the NASA MRPP.

## References

The following material is referenced in this document.

|  |  |
| --- | --- |
| **Document Title** | **Document Number** |
| NASA Enterprise Protection Program | NID 1058.127 |
| NASA Space Flight Program and Project Management Requirements | NPR 7120.5 |
| NASA Research and Technology Program and Project Management Requirements | NPR 7120.8 |
| NASA Space System Protection Standard | NASA-STD-1006 w/Change 1 |
| XXX Candidate Protection Strategy (CPS) Response Matrix (CRM) | N/A, *Dated*  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# executive summary

(U) Currently xx of the 16 CPS (revision 4.5) and yy of the 6 NASA-STD-1006 (w/change 1) requirements are being addressed by the project and their implementation is sufficient and verified by the XYZ Center Space/Mission Protection Team. VV of the CPS and ww of the Space System Protection Requirements (SSPR) remain TBD pending additional artifacts from the XXX project.

(U) The project office expects to deliver by TBD documentation that demonstrates the implementation is consistent with the corresponding strategies and responses provided by the project.

(U) ZZ protection-related risks have been identified and are being tracked in the XXX risk management system.

# PROTECTION PROCESS OVERVIEW

(U) The XYZ Center Space/Mission Protection Team is responsible for providing space asset protection related expertise, guidance and awareness for the XXX project. The XXX project will update the XXX PPP as necessary in advance of major project reviews and decision points. The XXX project will notify the XYZ Center Space/Mission Protection Team in advance of any configuration changes which could affect project compliance with Candidate Protection Strategies and NASA-STD-1006.

# XXX mission overview

(U) The following information was extracted and condensed from XXX project documents to provide context for this document only. The project-configured reference documents should be used for updated content accuracy and further details.

## XXX Program/Project Overview

<This section describes the programmatics of a mission.>

* <Discuss program/project organization, mission directorate, list stakeholders/customers>
* <Highlight heritage (e.g. previous flights)>
* <Describe mission class and risk category>

## XXX Mission Overview

<This section generally describes the purpose, scope and architecture of the mission to be protected.>

* <Top level mission objectives>
* <Orbit>
* <Science>
* <Space, Communications and Ground Segment overview>
* <Architecture Model (OV-1)>
* <CONOPS>

## Critical Project Technology (CPT) / Critical Project Information (CPI)

<List of the critical technologies and information that must be protected. CPI is defined in NASA-STD-1006, and CPS 6 and 7 provide additional context.>

# mission support elements

<List of the mission support elements (capabilities, services and infrastructure) provided by non-project institution(s) or program(s). Examples are communications networks (e.g. SN, DSN), ground systems (e.g. MCC, VAB, Range Safety), navigation and tracking systems (e.g. GPS), and enterprise-level cyber security. Normally, the relevant protections will be bundled with the mission support element and the expectation is that the project adopts/complies with the provided protections.>

# system criticality and susceptibilities

## Requirements

<List the level 2, 3 and 4 requirements that are relevant to project protection. In general these are the mission requirements used to assess compliance with the CPS.>

(U) Table 6-1 contains the driving Level 2 mission requirement from the XXX Mission Requirements Document that was used to assess the project CPS responses and compliance with NASA-STD-1006.

Table 6‑1. (U) Relevant Set of XXX Mission Requirements

| **MRD #** | **MRD Text** |
| --- | --- |
| MRD-xxx |  |
|  |  |

## Architecture

### Ground Segment Critical Elements and Susceptibilities

<This section identifies the critical elements within the ground segment and addresses the susceptibilities inherent in their design and operation. In this context, critical elements are those components of the (ground/communication/information/space) segment which are essential to the success of the mission and/or have particular protection-related susceptibilities. Susceptibilities are inherent weaknesses or limitations of a critical element which may be exploited by adversary actions.>

### Communication/Information Segment Critical Elements and Susceptibilities

<This section identifies the critical elements within the communication/information segment and addresses the susceptibilities inherent in their design and operation. See section 6.2.1 for a description of critical elements and susceptibilities.>

### Space Segment Critical Elements and Susceptibilities

<This section identifies the critical elements within the space segment and addresses the susceptibilities inherent in their design and operation. See section 6.2.1 for a description of critical elements and susceptibilities.>

## CONOPS

<This section identifies any protection-related processes in the mission CONOPS (e.g. contingency operations, continuity of operations, etc).>

# mission RISKS

<This section provides a space asset protection risk assessment to help the program/project prioritize mitigation strategies. The risk statements may be written in the format “Given <susceptibility>, if <trigger condition>, then <negative consequence>.” In order to rank a risk, both a probability and a consequence must be identified. In the case of space asset protection, level of effort for a potential adversary is typically used in place of probability of attack. Consequence is the impact on mission objectives if the risk is realized. Likelihood and Consequence scales should be normalized to match the “NASA Standard 5x5” (for an example see ESD-10003). Risks should be characterized using the template accompanying the “NASA Standard 5x5.”>

(U) Table 7-1 contains the ZZ protection risks for XXX as assessed by the program/project and the XYZ Center Space/Mission Protection Team with corresponding mitigation steps. The risks are based upon applicable threats, vulnerability details and additional risk context which are covered in Appendix C.

Table 7‑1. (U) XXX Top Protection Risks

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rank** | **ID / Trend** | **Title/Statement** | **Approach** | **Mitigation Steps** |
| 1(4x3) | 1🡺 | **Risk Title**Given AAA, if BBB, then CCC. | Mitigate | 1. Mitigation step #1
2. Mitigation step #2
 |

 |

When populated, the table may be SBU

**1**



# protection strategies

## Space System Protection Standard (NASA-STD-1006) Implementation

(U) Table 8-1 contains a summary of XXX project implementation of the Space System Protection Requirements (SSPR) in NASA-STD-1006. Currently yy of the 6 SSPRs are being addressed by the project and their implementation is sufficient and verified by the XYZ Center Space/Mission Protection Team. WW of the SSPR remain TBD pending additional artifacts from the XXX project. Appendix A provides the full assessment of XXX implementation of NASA-STD-1006.

<This section provides a stoplight table summary of NASA-STD-1006 implementation by the program/project. The program/project should indicate whether the SSPR is applicable and to what extent they intend to implement it. The XYZ Center Space/Mission Protection Team reviewer should indicate whether the program/project approach is sufficient. Possible responses could be “Yes”, “Partial”, “TBD”, “No”. The Notes section should identify key open items (e.g. outstanding artifacts) or departures (e.g. tailoring or waiving the requirement).>

**Table 8-1. (U) NASA-STD-1006 Implementation Summary for XXX**

| **SSPR #** | **SSPR** | **Recommended for Mission** | **Project Implementing** | **Current Implementation****Sufficiency** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| 1 | Programs/projects shall protect the command stack with encryption that meets or exceeds the Federal Information Processing Standard (FIPS) 140, Security Requirements for Cryptographic Modules, Level 1. |  |  |  |  |
| 2 | If a project uses an encrypted primary command link, any backup command link shall, at a minimum, use authentication. |  |  |  |  |
| 3 | The program/project shall protect the confidentiality of command link CPI as NASA sensitive but unclassified (SBU) information to prevent inadvertent disclosure to unauthorized parties per NASA Interim Directive (NID) 1600.55, Sensitive But Unclassified (SBU) Controlled Information, and NPR 2810.1, Security of Information Technology. |  |  |  |  |
| 4 | If project-internal PNT services are required, projects shall ensure that systems are resilient to the complete loss of, or temporary interference with, external PNT services. |  |  |  |  |
| 5 | Programs/Spectrum Managers/Operations Centers shall report unexplained interference to SAPP or to other designated notifying organizations. |  |  |  |  |
| 6 | Programs/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference. |  |  |  |  |

## Candidate Protection Strategies (CPS) Implementation

(U) Table 8-2 contains a summary of XXX project implementation of the CPS recommended by NASA MRPP, as of revision 4.5. Currently xx of the 16 CPS are being addressed by the project and their implementation is sufficient and verified by the XYZ Center Space/Mission Protection Team. VV of the CPS remain TBD pending additional artifacts from the XXX project. Appendix B provides the full assessment of XXX implementation of the CPS.

<This section provides a stoplight table summary of CPS implementation by the program/project. The program/project should indicate whether the CPS is applicable and to what extent they intend to implement it. The XYZ Center Space/Mission Protection Team reviewer should indicate whether the program/project approach is sufficient. Possible responses could be “Yes”, “Partial”, “TBD”, “No”. The Notes section should identify key open items (e.g. outstanding artifacts) or departures (e.g. program/project non-compliance).>

**Table 8-2. (U) CPS Implementation Summary for XXX**

| **CPS #** | **CPS** | **Recommended for Mission** | **Project Implementing** | **Current Implementation****Sufficiency** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| 1 | If encryption is selected as part of command link protection per NASA-STD-1006, has it been coordinated with the MRPP team and the NASA Communications Security (COMSEC) Central Office of Record (COR) early in the design process? |  |  |  |  |
| 2 | Will the saturation and damage thresholds of all on-board sensors be established prior to launch? |  |  |  |  |
| 3 | Are there telemetry monitoring capabilities on the ground or onboard to detect any unexpected conditions? |  |  |  |  |
| 4 | Have the failure analyses addressed maliciously induced effects across the mission architecture, assessing Ground, and Space segment fault, risk, and failure modes? |  |  |  |  |
| 5 | Have the Critical Project Information (CPI), Critical Project Technology (CPT), and Critical Components (CC) for Ground and Space segments been identified jointly with the MRPP? |  |  |  |  |
| 6 | Have all project documentation, media, information, and physical and electronic infrastructure (including facilities and equipment, and Flight and Ground Operations networks) been assessed to determine whether they contain Critical Project Information and Critical Project Technology and been correctly marked and protected as SBU? |  |  |  |  |
| 7 | Have the MRPP-provided procedures been incorporated into the CONOPS to report “suspicious” anomalies (e.g., tripped telemetry monitors, aberrant science) if unresolved, or if unexplained artifacts are discovered in post-processed (e.g., science and housekeeping) trending data? |  |  |  |  |
| 8 | Have hardware (backdoor) commands that could adversely affect mission success if used maliciously been identified and evaluated? |  |  |  |  |
| 9 | Has the reporting of “suspicious” anomalies been limited and controlled to only the community that has the need-to-know? |  |  |  |  |
| 10 | Has least access required for each role been enacted across the mission? |  |  |  |  |
| 11 | Have all external partner and internal agency network interconnections and data flows to/from the project boundary been documented and assessed to assure a commensurate protection level of information being processed? |  |  |  |  |
| 12 | Has the program/project considered how it will demonstrate the ability to promptly detect, report, mitigate, and recover from unauthorized activity within the operations center(s) and essential mission information flows? |  |  |  |  |
| 13 | Has an end-to-end risk assessment been performed for the entire mission thread and network interconnections?[Applies to both Space and Ground Systems.] |  |  |  |  |
| 14 | Does the ground system architecture incorporate network segmentation and isolation as appropriate? |  |  |  |  |
| 15 | Does the flight system architecture incorporate adequate protections at the interfaces between components and subsystems to limit propagation of anomalous conditions? |  |  |  |  |
| 26 | Is the system protected, any segment and any source, from improper or invalid input? |  |  |  |  |

# Abbreviations and acronyms

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| MRPP | Mission Resilience and Protection Program |
|  |  |
|  |  |

Appendix A – NASA-STD-1006 Implementation for XXX

(U) The following section addresses XXX project implementation of the requirements in NASA-STD-1006 (w/change 1). For each Space System Protection Requirement (SSPR), the following items are included:

* The project response for (planned) implementation. The response should expand on any approach other than full implementation to indicate if the requirement was waived, tailored, or only partially implemented.
* Artifact(s) inspected demonstrating implementation
* Analysis of the response in the context of the mission. The analysis should be provided by, or at least coordinated with, the XYZ Center Space/Mission Protection Team reviewer of the PPP.

SSPR 1: Programs/projects shall protect the command stack with encryption that meets or exceeds the Federal Information Processing Standard (FIPS) 140, Security Requirements for Cryptographic Modules, Level 1.

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of SSPR:***

SSPR 2: If a project uses an encrypted primary command link, any backup command link shall, at a minimum, use authentication.

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of SSPR:***

SSPR 3: The program/project shall protect the confidentiality of command link CPI as NASA sensitive but unclassified (SBU) information to prevent inadvertent disclosure to unauthorized parties per NASA Interim Directive (NID) 1600.55, Sensitive But Unclassified (SBU) Controlled Information, and NPR 2810.1, Security of Information Technology.

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of SSPR:***

SSPR 4: If project-internal PNT services are required, projects shall ensure that systems are resilient to the complete loss of, or temporary interference with, external PNT services.

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of SSPR:***

SSPR 5: Programs/Spectrum Managers/Operations Centers shall report unexplained interference to SAPP or to other designated notifying organizations.

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of SSPR:***

SSPR 6: Programs/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of SSPR:***

Appendix B – CPS Implementation Table for XXX

(U) The following section addresses the Candidate Protection Strategies (CPS), version 4.5, recommended by NASA MRPP for Flight Programs and Projects. For each CPS, the following items are included:

* Applicability/efficacy of the CPS as related to this mission. The project indicates whether the CPS is applicable to XXX.
* The project response for (planned) implementation. The response should expand on any approach other than full implementation to indicate partial or incomplete implementation.
* Analysis of the response in the context of the mission. The analysis should be provided by, or at least coordinated with, the XYZ Center Space/Mission Protection Team reviewer of the PPP.

### B.1.1 Engineering Focused Strategies — Space Segment

CPS-1: If encryption is selected as part of command link protection per NASA-STD-1006, has it been coordinated with the MRPP team and the NASA Communications Security (COMSEC) Central Office of Record (COR) early in the design process?

***Project Applicability/Efficacy:*** *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-2: Will the saturation and damage thresholds of all on-board sensors be established prior to launch??

***Project Applicability/Efficacy:*** *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

### B.1.2 Engineering Focused Strategies — Ground Segment

CPS-3: Are there telemetry monitoring capabilities on the ground or onboard to detect any unexpected conditions?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-4: Have the failure analyses addressed maliciously induced effects across the mission architecture, assessing Ground, and Space segment fault, risk, and failure modes?

***Project Applicability/Efficacy:*** *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

### B.1.3 Engineering Focused Strategies — All Segments

CPS-5: Have the Critical Project Information (CPI), Critical Project Technology (CPT), and Critical Components (CC) for Ground and Space segments been identified jointly with the MRPP?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-6: Have all project documentation, media, information, and physical and electronic infrastructure (including facilities and equipment, and Flight and Ground Operation networks) been assessed to determine whether they contain CPI or CPT and been correctly marked and protected as SBU?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

### B.2 CONOPS Focused Strategies

CPS-7: Have the MRPP-provided procedures been incorporated into the CONOPS to report “suspicious” anomalies (e.g., tripped telemetry monitors, aberrant science) if unresolved, or if unexplained artifacts are discovered in post-processed (e.g., science and housekeeping) trending data?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-8: Have hardware (backdoor) commands that could adversely affect mission success if used maliciously been identified and evaluated?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-9: Has the reporting of “suspicious” anomalies been limited and controlled to only the community that has the need-to-know?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

### B.3.1 Cyber Focused Strategies — Access

CPS-10: Has least access required for each role been enacted across the mission?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-11: Have all external partner and internal agency network interconnections and data flows to/from the project boundary been documented and assessed to assure a commensurate protection level of information being processed?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

***Analysis of Response/Implementation of CPS:***

CPS-12: Has the program/project considered how it will demonstrate the ability to promptly detect, report, mitigate, and recover from unauthorized activity within the operations center(s) and essential mission information flows?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

### B.3.2 Cyber Focused Strategies — System Design

CPS-13 Has an end-to-end risk assessment been performed for the entire mission thread and network interconnections? [Applies to both Space and Ground systems.]

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-14: Does the ground system architecture incorporate network segmentation and isolation as appropriate?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

CPS-15: Does the flight system architecture incorporate adequate protections at the interfaces between components and subsystems to limit propagation of anomalous conditions?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***

### B.3.3 Cyber Focused Strategies — Software Design

CPS-16: Is the system protected, any segment and any source, from improper or invalid input?

*Project Applicability/Efficacy:* *Recommended for this mission.*

***Project Response:***

***Artifacts Inspected:***

***Analysis of Response/Implementation of CPS:***