NASA Mission Resilience and Protection Program

Candidate Protection Strategies

MRPP.CPS.20201216
Version 4.5

December 16, 2020

DOCUMENT HISTORY LOG

STATUS	REVISION	EFFECTIVE DATE	DESCRIPTION
INIT	-	December 4, 2015	Initial Release
Update	V2	June 6, 2016	Added CPS 28 and 29
Update	V3	July 30, 2018	Deleted or combined redundant or unnecessary strategies
Update	V4	November 4, 2019	Added cybersecurity strategies
Update	V4.5	December 16, 2020	Deleted strategies addressed in NASA-STD-1006, administrative program name change from SAPP to MRPP

AUTHORITY

These Candidate Protection Strategies (CPSs) are promulgated under the authority of NASA's Mission Resilience and Protection Program (MRPP), and should be used by civil space missions as guidelines in generating their Project Protection Plans (PPP). CPS and PPP training is available from the MRPP.

SCOPE

This document defines CPSs as guidelines for US civil space flight missions, and suggests protective measures that could be taken to implement the strategies in order to mitigate possible threats to mission success.

To a great degree, the CPSs overlap with good systems engineering. The intent of the strategies is to expand the typical system engineering domain to include the unique challenges presented by specific threats to space missions. Each program/project should consider what an adversary could do/has done to degrade or deny use of a mission, what external event(s) could affect mission success, and then identify reasonable steps to mitigate them.

The CPSs include selected cybersecurity strategies to help missions address emerging space cybersecurity challenges. The cybersecurity strategies were selected in particular to assist missions in enhancing their cybersecurity resilience for command and control, mission operations centers and external interfaces. These strategies also complement the cybersecurity control documentation noted in System Security Plans (SSP).

APPLICABILITY

These strategies are applicable to all space flight missions; from hosted payloads to full satellites, crewed vehicles, and all flight platforms, including their ground systems, flight management and operations, mission data processing, and communication networks, from design definition and implementation, through operations and disposal. Certain CPS may have limited or no applicability for a particular program/project. For instance, hosted instrument projects are only responsible for the protection of transmitted instrument commands until they are received by the host spacecraft operations center.

COMPLIANCE

While in principle the strategies apply to all missions, compliance is to be determined on a case-by-case basis by the program/project manager, and approved by Center Technical Authority and the appropriate Mission Directorate representative, as part of the PPP.

The strategies are to be reviewed and evaluated with respect to: a) the threat environment for that mission, program or project as defined by the MRPP, b) the mission's risk posture and classification, and c) the specific mission's role in the overall civil space mission. All missions are expected to coordinate with a MRPP representative on matters of interpretation and applicability of the strategies. In practical terms, some science missions such as PI-led (AO) missions, hosted payloads, and instruments-of-opportunity, may find full compliance unnecessary if sufficient justification is provided to support less than full compliance. Conversely, mature aerospace organizations will likely find compliance with the strategies just the normal course of business as part of standard engineering or business practices, with little or no extra effort.

The degree of planned or actual mission compliance for each strategy is to be documented in the PPP, including a brief description of the implementation approach, and justification for any non-compliances. Formal waiver requests for the CPS are not required.

Programs/projects shall comply with NASA Information Technology (IT) security requirements and complete SSPs in accordance with NPR 2810.1. Compliance with the cybersecurity CPS is complementary to, rather than a substitute for, institutional IT security practices and documentation.

Applicable reference sources are listed in Appendix A as supporting material. Appendix B is a lexicon of abbreviations and terms used in the strategies and mitigation steps.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
Engineering Focused Strategies — Space Segment	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?	Coordinating encryption means the NIST- or NSA-compliant implementation should be coordinated with the MRPP and the NASA COR, for a range of security protocols (e.g., the encryptor/decryptor implementation, key generation, key management, key distribution, testing, and pre- and post-launch physical security). The MRPP will aid in coordinating with the NASA COR in the Office of Protective Services
	2	Will the saturation and damage thresholds of all on-board sensors be established prior to launch?	The electro-magnetic sensitivities of all RF and optical apertures should be evaluated and established with respect to any applicable characteristics such as: Fields-Of-View, in-band and out-of-band wavelengths/frequencies, minimum dwell times to saturation and damage, minimum energy to saturation and damage, pointing agility, shutters (including reaction/activation time and recovery time) and sensitivity to direct sun exposure. The MRPP will use these thresholds to advise of new threats that arise over the mission life.
Engineering Focused Strategies — Ground Segment	3	Are there telemetry monitoring capabilities on the ground or onboard to detect any unexpected conditions?	Unexpected conditions can include RF lock-ups, loss of lock, failure to acquire an expected contact and unexpected reports of acquisition, failure to acquire GPS satellites, unusual AGC and ACS control excursions, unusual navigation or timing behavior, unforeseen actuator powering or actions, thermal stresses, power aberrations, failure to authenticate, software or counter resets, etc. Mitigation might include additional telemetry monitor flags, specific AGC and PLL thresholds to alert operators, auto-capturing state snapshot images in memory when unexpected conditions occur, signal spectra measurements, and expanded default diagnostic telemetry modes to help in identifying and resolving anomalous conditions.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
	4	Have the failure analyses addressed maliciously induced effects across the mission architecture, assessing Ground, and Space segment fault, risk, and failure modes?	The mission-specific threats can be used to generate an assessment of how the overall architecture would react to each threat and what the indicators would be. Consider if new system-level risks are identified by the aggregation of heritage and newly developed system characteristics. The assessments should be coordinated with the appropriate stakeholders: for example implementation and I&T organizations, scientists, operators, etc., to ensure the indicator(s) will be identified as a threat response, and reported correctly.
Engineering Focused Strategies — All Segments	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?	During each phase of the mission development, the project should identify the mission-specific critical category items jointly with the MRPP; the MRPP will then coordinate distribution throughout the protection community, and provide feedback to the project on any additional or suggested criticalities. Critical Project Information and Critical Project Technology are items which, if compromised or otherwise inappropriately disclosed, could put mission success at risk or provide an adversary an advantage. Critical Components include hardware, software, and firmware which delivers or protects the mission critical functionality of a system.
	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?	Coordinate with the MRPP and the supporting Center's Chief Information Security Officer (CISO) office to interpret the requirements in NPR 2810, *Security of Information Technology*, for marking and protection, and to apply them to the specific mission against known threats.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
ConOps Focused Strategies	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?	In coordination with the MRPP, identify specific criteria for "suspicious" (potentially malicious) anomalies and unexplained excursions in post-processed mission data, and generate procedures for timely reporting. Evolve the criteria during flight to minimize false positives.
	8	Have hardware (backdoor) commands that could adversely affect mission success if used maliciously been identified and evaluated?	Coordinate with the MRPP to confirm that only hardware commands for the purpose of providing emergency access are being used, and that commanding authority is appropriately restricted, eliminating as many such unnecessary commands as is practical. Test commands not needed for flight should be deleted or disabled.
	9	Has the reporting of “suspicious” anomalies been limited and controlled to only the community that has the need-to-know?	This is to avoid providing feedback to an adversary about the effects of their interventions.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
Cyber Focused Strategies — Access	10	Has least access required for each role been enacted across the mission?	Limit access (authentication and authorization) to systems, resources and data to only that required for the role. Detect and respond to insider threat and unauthorized elevated privileges. Limit adverse consequences in the event of network penetration. Use a risk-based approach to implement access controls (e.g., two-factor PIV authentication or other IAL3/AAL3 credential) commensurate with mission needs.[1]
	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?	Ensure inherent risk to NASA mission systems as well as risk to NASA mission data are understood, documented, and approved. For the purpose of mission assurance, ensure all interconnections coming from outside of the project (even within the agency) have appropriate network segmentation. Ensure external partners and supporting agency systems processing sensitive NASA data have adequate protections in place. At a minimum, these protections are documented in Interconnection Security Agreements that reference the implemented security controls allocated to that interface. Interconnections includes individual remote connections (RDP, VPN, etc.) and requires approval of Authorizing Official. The project boundary encompasses all assets under direct project control. Protections for interconnections include multi-factor authentication, least privilege-based access controls, network segmentation, secure remote access protocols, and managed interconnections.

[1] "Cyber Resilient Flight Software for Spacecraft," Wayne Wheeler, Nicholas Cohen and Joseph Betser, Aerospace Corporation presentation, 12-14 September 2017.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
	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?	Maintain sufficient awareness of normal operations, network, and IT system performance so that anomalous behavior or unauthorized activity can be rapidly identified and managed. Unauthorized activity is a superset of malicious activity such as a network intrusion. The program/project should identify its essential operations processes and systems. For the identified elements, ensure that a sufficient transaction history is stored for trending and historical analysis, a capability to monitor for signs of unauthorized activity is in place and tested, and alerts are relayed to appropriate parties for review and action. Essential operations processes may include command load generation, ground system configuration management (e.g., updates/changes), and cryptographic key management. Essential systems may include the operations physical access control, console operator authentication/logon/ logoff records, network interfaces to the operations areas, and associated internal IT services. Program/project should work with the various appropriate cybersecurity teams to a common understanding on identifying anomalous or unauthorized activity, sharing/relaying of data including alerts, and testing to ensure capabilities are functioning as intended.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
Cyber Focused Strategies — System Design	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]	Select critical mission threads for analysis. Identify supporting infrastructure and associated security controls. Include elements outside direct project control if the mission depends on these elements. Identify known vulnerabilities associated with the mission. Characterize feasible attacks. Assess the likelihood and potential impact of successful exploits. Propose mitigations to address the risks. This process should be done on a continual basis, including at all KDPs.[2] Cyber risks from all elements of the end-to-end architecture should be evaluated on a continuous basis throughout the project lifecycle, including during operations. Recommend that projects work with the supporting Center's CISOs to conduct risk assessments in accordance with NIST guidance (NIST publications contain risk assessment guidance beyond sole vulnerability assessments) and to integrate cyber risks into project risk management.
	14	Does the ground system architecture incorporate network segmentation and isolation as appropriate?	Identify the ground components that will be communicating and the data flows of this communication as well as specifics such as method/protocol and port/address. Ensure communications are isolated to only the components that need to communicate with one another.
	15	Does the flight system architecture incorporate adequate protections at the interfaces between components and subsystems to limit propagation of anomalous conditions?	Identify the flight components that will be communicating and the data flows of this communication as well as specifics such as method/protocol. Ensure communications are isolated to only the components that need to communicate with one another.

[2] "Threats Driven Cyber Resilience," Aerospace Corporation presentation, February 9, 2018.

Strategy Focus	CPS#	Candidate Protection Strategy (CPS)	Candidate Mitigation Steps/Rationale
Cyber Focused Strategies — Software Design	16	Is the system protected, any segment and any source, from improper or invalid input?	Primary focus is on the system command path, critical dependencies (e.g., PNT), and logic supporting key performance parameters. Consider internal and external system boundaries. Input errors can be due to a command errors, bit flips in the channel, software errors, etc. Errors can also be due to deliberate manipulation or spoofing. Timing of input signals, if varied in an unexpected manner, may also trigger undesirable effects in the system.[3] Test for good software hygiene, including assessment of software security controls, code analysis, and ongoing vulnerability scanning. Test plans should include deliberately malformed data input, including representative edge cases. Apply whitelists for valid data ranges when possible.

[3] "Cyber Resilient Flight Software for Spacecraft"

APPENDIX A

APPLICABLE REFERENCE SOURCES

CPS	APPLICABLE & REFERENCE SOURCES
All	NASA Engineering Network; Space Asset Protection https://nen.nasa.gov/web/sap NASA Online Directives Information System – Useful Links http://nodis3.gsfc.nasa.gov/links_lib.cfm MRPP NASA-DL-MRPP@mail.nasa.gov
1	MRPP-specific guidelines
2	
3	
4	
5	
6	NPD 1600.2, *NASA Security Policy* NPR 2200.2, *Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information* NPR 2810.1, *Security of Information Technology* NPR 1600.1, *NASA Security Program Procedural Requirements* NPD 2810.1, *NASA Information Security Policy* NPR 1620.2, *Facility Security Assessments* NPR 1620.3, *Physical Security Requirements for NASA Facilities and Property* NPR 7120.9 *Product Data & Life Cycle* ITCD Data at Rest: http://itcd.hq.nasa.gov/DAR.html
7	MRPP-specific guidelines
8	
9	
10	NIST SP 800-171 Rev.1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* NIST SP 800-12 Rev.1 under Least Privilege, *An Introduction to Information Security* NIST SP 800-57 Part 2 under Least Privilege, *Recommendation for Key Management* NASA IT Security Handbook 2810.09 – Incident Response
11	NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
12	NASA IT Security Handbook 2810.09 – Incident Response
13	MRPP-specific guidelines
14	
15	
16	Common Weakness Enumeration (CWE) Category: Validate Inputs https://cwe.mitre.org/data/definitions/1019.html

APPENDIX B

LEXICON OF ABBREVIATIONS & TERMS

Appendix B
Lexicon of Abbreviations and Terms

ACRONYM	DEFINITION	USED	MEANING
ACS	Attitude Control Subsystem	CPS 3	An assemblage of sensors, actuators, and software that establishes, controls, and reports the orientation of a satellite with respect to a given reference frame. Also known as Attitude Determination and Control Subsystem.
AGC	Automatic Gain Control	CPS 3	Engineering term for circuitry with feedback that adjusts the output level as a function of the input.
AO	Announcement of Opportunity	P. 1	Procurement vehicle for the NASA Science Mission Directorate
	Backdoor Commands	CPS 8	Residual commands used for board/box/unit development/acceptance testing, or supplemental vendor commands that execute operating modes outside the mission scope, which have not been included in the flight command database, but would still be executed with unforeseeable results, if sent to the spacecraft.
	Coordinate with MRPP	CPS 1,5,6,8	Provide situational information to MRPP in an agreed upon timeliness and format, and subsequently engaging in dialogue and information exchange to reach a mutually agreeable course of action to clarify and resolve the situation.
COR	Central Office of Record	CPS 1	Organization that performs basic key and Communications Security management functions, such as key ordering, distribution, inventory control, etc.
	Critical Components	CPS 5	Hardware, software, and firmware which delivers or protects the mission critical functionality of a system.
	Critical Project Information	CPS 5,6	Data, descriptive text, algorithms, source code, drawings, operational timelines, or parameters about a system design, application or performance, which if it were compromised or otherwise inappropriately disclosed, could put the mission success at risk or provide an adversary an advantage.
CPS	Candidate Protection Strategy	throughout	Numbered list of possible design, institutional, and operational steps to consider as threat mitigation
	Critical Project Technology	CPS 5,6	Hardware or software applied in practice or design to accomplish a mission, which if its procurement, implementation, performance, or lifetime were

Appendix B
Lexicon of Abbreviations and Terms

ACRONYM	DEFINITION	USED	MEANING
			compromised, would put the mission success at risk or provide an adversary an advantage.
	Direct Project Control	CPS 11, 13	Entities which are directly accountable to the project on either a temporary or permanent basis for their configuration and performance.
	External Partner Interconnections	CPS 11	External, non-NASA entities who operate a third-party system outside NASA's network which requires an interconnection to a NASA-owned network in order to conduct business.
GPS	Global Positioning System	CPS 3	A satellite navigation system that provides location and time information in all weather conditions.
	Hardware Commands	CPS 8	Spacecraft commands that, once extracted by the spacecraft from the uplink command channel, are routed to a specific location and are executed on receipt, without any manipulation, timing or parameters provided by the spacecraft.
IAL3/AAL3	Identity Assurance Level 3 / Authentication Assurance Level 3	CPS 10	The National Institute of Standards and Technology Special Publication 800-63, Digital Identity Guidelines, establishes different assurances levels (1–3, in order of least to most secure, as options for implementation based on an organization's risk profile). IAL refers to the identity proofing process. Organizations determine IAL based on the potential harm caused by an attacker making a successful false claim of an identity. AAL refers to the authentication process. Organizations determine AAL based on the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems.
	Least Privilege	CPS 11	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
MRPP	Mission Resilience and Protection Program	throughout	An effective organization which identifies threats to civil space missions, and suggests ways to mitigate the risk to mission success. Current trends in technology proliferation, accessibility to space, globalization of space programs and industries, commercialization of space systems and services,

Appendix B
Lexicon of Abbreviations and Terms

ACRONYM	DEFINITION	USED	MEANING
			and foreign knowledge about U.S. space systems increase the likelihood that U.S. space systems may come under attack, particularly vulnerable systems. Contact NASA MRPP via NASA-DL-MRPP@mail.nasa.gov.
NIST	National Institute of Standards and Technology	CPS 1,13	The federal technology agency that works with industry to develop and apply technology, measurements, and standards
NSA	National Security Agency	CPS 1	The organization that protects U.S. national security systems, and produces foreign signals intelligence information.
PI	Principal Investigator	Intro	The ultimate authority selected to be responsible for a certain type of civil space mission.
PIV	Personal Identity Verification	CPS 10	PIV is a common credentialing and standard background investigation process required by Homeland Security Presidential Directive 12 (HSPD-12). A PIV card is a United States smartcard that contains the necessary data for the cardholder to be granted access to federal facilities and information systems and assure appropriate levels of security for all applicable federal applications
PLL	Phase Lock Loop	CPS 3	Engineering term for circuitry with feedback that adjusts the frequency or gain output as a function of the phase of the input frequency.
PNT	Pointing, Navigation & Timing	CPS 16	Generic term for the information to carry out these activities.
RF	Radio Frequency	CPS 2,3	Electromagnetic energy between 3 kHz and 300 GHz.
SBU	Sensitive But Unclassified	CPS 6	Restricted access information (to be replaced by *Controlled Unclassified Information* (CUI) per Executive Order 13556).