National Aeronautics and Space Administration

NASA STD-1006: Space System Protection Requirements

Presented to the Small Spacecraft Systems Virtual Institute (S3VI) by

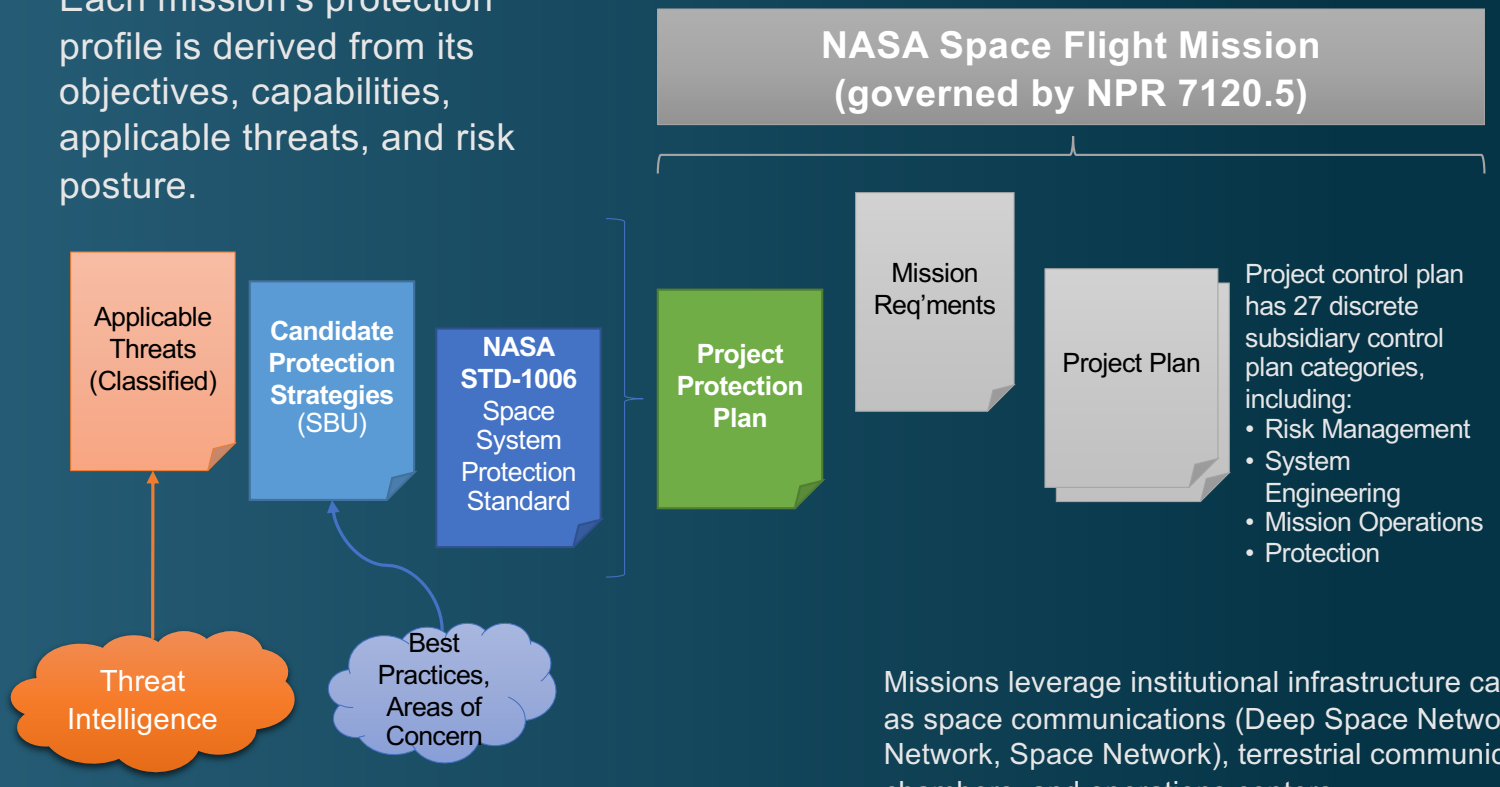
Joshua.Krage@nasa.gov and
David.E.Adams@nasa.gov

2020-11-18

NASA Office of the Chief Engineer
Mission Resilience and Protection Program (renamed from the Space Asset Protection Program in March 2020)

Space Protection Approach

Each mission's protection profile is derived from its objectives, capabilities, applicable threats, and risk posture.



Missions leverage institutional infrastructure capabilities, such as space communications (Deep Space Network, Near Earth Network, Space Network), terrestrial communications, test chambers, and operations centers.

NASA Protection Guidance, Summary

Highlighted items are new since last briefing

NASA Enterprise Protection Guidance

- NPR 1058.1, June 2019, NASA Enterprise Protection Program
  - Establishes the roles and responsibilities for the Principal Advisor for Enterprise Protection, the Enterprise Protection Program (EPP), and the Enterprise Protection Board (EPB)
- NID 1058.127, May 2020
  - NASA program/projects started after February 1, 2019 shall implement NASA-STD-1006
  - Existing program/projects shall determine, in coordination with OCE, which requirements to implement

NASA Space Protection Guidance

- NPR 7120.5, August 2012 / March 2020 (Change 18), NASA Space Flight Program and Project Management Requirements w/ Change 18
  - Requires a project protection plan that incorporates inputs from threat intelligence, Candidate Protection Strategies, and applicable standards
- NID 7120.130, July 2020, NASA Space Flight Program and Project Management Requirements - Space Systems Protection Standard Update
  - Requires protection plans to address STD-1006
- NPR 7120.8 , September 2018 (amended August 2020), NASA Research and Technology Program and Project Management Requirements
  - Requires research and technology projects operating in space to implement a protection plan
- Candidate Protection Strategies v4 (SBU)
  - Starting point for developing a protection plan, series of questions related to best practices to mitigate high threat and risk issues
- NASA-STD-1006 w/ Change 1: Space System Protection Standard
  - Baseline standards to improve space system protection from well understood threats

Note also: related guidance for physical/industrial security (NPD 1600 series), and information security (NPD 2810 series)

NASA Engineering Network (NEN) Mission Resilience and Protection Community of Practice site:

- https://nen.nasa.gov/web/sap

Background and Context

Path to the Standard

- OCE directed SAPP (*now MRPP*) in July 2018 to incorporate the requirements in a technical standard
  - Initiated NASA-STD-1006, “Space Asset Protection Standard” in October 2018
  - Standard release for Agency comments on 17 Oct 2018
  - All comments reconciled after multiple review cycles
- NASA Chief Engineer approved NASA-STD-1006 on 29 Oct 2019, and first change approved 5 Nov 2020
  - Download: https://standards.nasa.gov/standard/oce/nasa-std-1006-wchange-1
- Mandatory use established in NID 1058.127, May 2020
  - Requires all programs/projects established after 1 Feb 2019 to comply with NASA-STD-1006
  - For programs/projects established prior to 1 Feb 2019, PMs shall determine with OCE which NASA-STD-1006 requirements to implement
  - Effectively supersedes AA Memo from February 2019

Context [1]

- Agency-level protection requirements are intended to ensure NASA missions are resilient to threats
- Resilience to threats is needed to reduce the risk of adverse consequences to the Agency
- Primary consequences include and are not limited to:
  - Inability to satisfy mission requirements
  - Risk to human safety
  - Loss of control of a civil space asset
  - Damage to NASA's reputation

Context [2]

- Representative set of threat actions below reflects emerging counterspace threats to a wide range of civil space missions:
  - Command link jamming – sufficient RF energy directed at the spacecraft in its command link frequency may preclude the ability to receive commands during the period of RF emissions.
  - Command link intrusion – valid commands with proper encryption or authentication injected within the command path may lead to a temporary or permanent loss of control.
  - GPS jamming – sufficient RF energy directed at the spacecraft at GPS signal frequencies may preclude the spacecraft GPS receiver from receiving GPS signals during the period of RF emissions.
  - GPS spoofing – RF energy directed at the spacecraft at GPS signal frequencies with selected phasing may alter the navigation and timing solution of the spacecraft during the period of RF emissions.
  - Cyber exploitation of critical project technologies (CPT) and critical project information (CPI) – adversary acquisition and use of CPT/CPI may enable the adversary to overcome system protections and induce harm to the system or to manipulate science data.

Context [3]

- Requirements are established at an Agency level
  - Protection against the consequences are needed because they convey risk to the Agency and to the US space enterprise.
  - Requirements are intended to decrease the likelihood of an adversary in achieving success and to increase the likelihood of detecting threat actions against NASA systems
  - The requirements establish the minimum space protection posture expected of all NASA programs/projects of record
- Additional program/project-specific protection requirements may be added to these Agency requirements
  - As needed to address dynamic threats and a changing threat environment
  - To address Project unique vulnerabilities

Requirements

4.1.1 Command Stack Protection

Requirement	Tailoring	Guidance	CPS
SSPR 1: Programs/projects shall protect the command stack with encryption which meets or exceeds the Federal Information Processing Standard (FIPS) 140, **Level 1**.	1. Hosted instruments only require protection of instrument command stack. 2. Hosted instruments are only responsible for protection of command stack until host spacecraft operations center receives commands. This protection may be provided either via encryption (preferred) or authentication. 3. Deep space missions may choose to limit controls applied to the space link if certain controls pose significant burden to operability or mission success, and if the threat to the space link is low. 4. Cat 3/Class C or Class D missions may authenticate without encryption if they have no propulsion. **5. This requirement does not apply to balloon or sounding rocket projects.**	1. Missions should pursue multiple protections as a defense in depth measure; **therefore, missions should implement both encryption and authentication to the extent possible.** 2. Missions can select an appropriate encryption scheme for each leg of the command path, e.g., SOC -> MOC -> Tracking Station -> Spacecraft 3. Crewed missions should also protect intra-vehicle and intra-suit communications 4. Missions should protect the integrity of the command generation process 5. Missions using CCSDS should consult CCSDS350.0-G, CCSDS 355.0-B and CCSDS 352.0-B. Note that FIPS 140 compliance meets and exceeds the cryptographic specifications of CCSDS 352.0-B. **All missions should implement CCSDS 232.1-B-2, COP-1; but by itself CCSDS 232.1-B-2 is insufficient to meet this requirement.**	1, 2

Rationale:

- Command link incidents with civil space missions have demonstrated potential impacts to safe operations. Additionally, NASA end of mission (EOM) experiments found that spacecraft without encryption or authentication are particularly susceptible to these impacts.

4.1.2 Backup Command Link Protection

Requirement	Tailoring	Guidance	CPS
SSPR 2: If a project uses an encrypted primary command link, any backup command link shall at minimum use authentication.			1

Rationale:

- Missions need to balance command authority with command integrity and the ability to recover from an anomalous condition. Additionally, command link contingency modes need protection from malicious actors.

4.1.3 Command Link Critical Program/Project Information (CPI)

Requirement	Tailoring	Guidance	CPS
SSPR 3: The program/project shall protect the confidentiality of command link CPI as NASA SBU information to prevent inadvertent disclosure to unauthorized parties per NID 1600.55 and NPR 2810.1.		1. The **MRPP** can assist the program/project with command link CPI identification. 2. CPI may include sensitive command information such as hardware commands, key handling/management, and bit patterns of critical commands.	6, 7

Rationale:

- Command link incidents with civil space missions have demonstrated potential impacts to safe operations. Command link CPI protection is part of a defense in-depth approach to command link protection, encompassing encryption, authentication, and CPI protection.

4.2.1 Ensure Positioning, Navigation and Timing (PNT) Resilience

Requirement	Tailoring	Guidance	CPS
SSPR 4: If project-external PNT services are required, Projects shall ensure that systems are resilient to the complete loss of, or temporary interference with, external PNT services.		1. PNT filtering algorithms that blend high-fidelity models of orbital dynamics and/or a diversity of measurement sources have been proven in flight operations to detect and survive interference. NASA/TP-2018-219822 describes NESC Best Practices for navigation filter design. 2. PNT computations should be tested for resiliency to invalid parameter inputs, e.g. as in the current version of GPS interface specification IS-GPS-200. 3. Projects should have a plan for emergency backup independent PNT sources that is appropriate to the mission's risk tolerance and cost-benefit posture. Backup implementations involving either the mission's space segment or ground segment are possible. **Projects should consider verifying PNT pre-flight performance to demonstrate the spacecraft does not enter an unacceptable mode when PNT inputs change or are interrupted.** 4. Nominally the emergency backup plan is only intended to enable spacecraft survival. Projects whose mission requirements necessitate that the spacecraft continue to perform the mission (i.e., still meet the minimum Level 1 requirements) while operating in the face of denial or manipulation of the primary PNT source will need to address such considerations in their planning and possibly incorporate design features in the flight or ground hardware to provide for backup PNT capabilities. 5. Missions requiring PNT services should also consult NPD 8900.4 "NASA Use of Global Positioning System Precise Positioning Service."	12,13

Rationale:

- Per www.gps.gov, PNT systems are subject to interference from both natural and human-made sources.

4.3.1 Interference Reporting

Requirement	Tailoring	Guidance	CPS
SSPR 5: Projects/Spectrum Managers/Operations Centers shall report unexplained interference to **MRPP** or to other designated notifying organizations.		1. Hosted instruments need only monitor indigenous telemetry and mission data. 2. Missions should incorporate autonomous telemetry monitoring to support operational teams in the detection of unexpected command link energy, unexpected loss of GPS satellite solutions, and other unexplained interference events. 3. Missions should incorporate procedures for operations teams to contact NASA **MRPP** in case of unexpected command link energy, unexpected loss of GPS satellite solutions, or any unexplained interference event. The intent here is for only suspected purposeful interference to be reported. 4. This requirement may be implemented in either the space segment or the ground segment. 5. In the absence of a designated notifying organization, contact NASA **MRPP via NASA-DL-EMI-REPORT@mail.nasa.gov**. 6. This requirement does not replace other reporting or notification requirements, such as to the NASA spectrum managers (see NPR 2570.1, “NASA Radio Frequency (RF) Spectrum Management Manual.”)	4, 8, 9

Rationale:

- Command link and GPS degradation/disruption incidents can potentially impact the safe operation of civil space missions. Additionally, NASA has the responsibility to report unexpected interference with command links and GPS signals to other Federal agencies in compliance with the charter of the Purposeful Interference Response Team and with the National Space Policy.

4.3.2 Interference Reporting Training

Requirement	Tailoring	Guidance	CPS
SSPR 6: Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.		1. Missions should conduct training annually, as a minimum, using the latest reporting procedures	8, 9

Rationale:

- Command link incidents with civil space missions have demonstrated potential impacts to safe operations. These incidents can be easily missed if operators are not aware of, or focusing on, the characteristics of adversarial intrusions. Additionally, GPS incidents with civil space missions have shown that missions can unexpectedly lose GPS signals. Furthermore, NASA has the responsibility to report unexpected interference with command links and GPS signals to other Federal agencies. Finally, the dynamic nature of the threat environment and operations team turnover necessitate annual proficiency training.

Takeaways

- NASA-STD-1006 w/ Change 1 is ready for use
  - Crafted to encompass the building blocks of civil space system protection
  - Leverages Federal and International standards and best practices

- Requirements are structured to permit flexibility
  - Minimizes specific implementation direction, allowing the mission to select more specific requirements

Provides a foundational level of protection that is consistent across NASA

Backup Slides

Protection Plan Content Breakout

- Protection Plan
  - Project/mission background
  - Protection-related requirements
  - Susceptibilities
  - Risk assessment
  - NASA-STD-1006 assessment
  - Candidate Protection Plans assessment
- Appendix C
  - Threat applicability
  - Threat summary
  - Vulnerability analysis
  - Detailed risk analysis
  - Mitigation recommendations

- Document is normally controlled as NASA Sensitive But Unclassified (SBU).
- Appendix C contents are normally Classified due to content.

Candidate Protection Strategies (CPS) v4

- Serve as a starting point for mission protection planning
- Best practices, consider relevant threat intelligence and risk issues
- Protection plans incorporate results of the CPS analysis, including any requisite requirement tailoring

Main Categories (# of questions)

1. Engineering Focused Strategies – Space Segment (3)
2. Engineering Focused Strategies – Ground Segment (2)
3. Engineering Focused Strategies – All Segments (2)
4. ConOps Focused Strategies (6)
5. Cyber Focused Strategies – Access (3)
6. Cyber Focused Strategies – System Design (3)
7. Cyber Focused Strategies – Software Design (1)

CPS document is NASA Sensitive But Unclassified (SBU), available:
- via the NASA Engineering Network (NEN) SAP community of practice site (in the SBU folder), or
- via request from the NASA MRPP team

NASA Technical Standard NASA-STD-1006 **w/ Change 1**
Space System Protection Standard [approved 2019-10-29, updated 2020-11-05]

Highlighted phrases are updates from the prior version

NOT MEASUREMENT SENSITIVE

NASA TECHNICAL STANDARD

Office of the NASA Chief Engineer

NASA-STD-1006 w/CHANGE 1: ADMINISTRATIVE/ EDITORIAL CHANGE 2020-11-05

Approved: 2019-10-29

SPACE SYSTEM PROTECTION STANDARD

APPROVED FOR PUBLIC RELEASE—DISTRIBUTION IS UNLIMITED

Maintain Command Authority

- Command Stack Protection: Programs/projects shall protect the command stack with encryption that meets or exceeds the FIPS 140, Level 1.
- Backup Command Link Protection: If a project uses an encrypted primary command link, any backup command link shall at minimum use authentication.
- Command Link Critical Program/Project Information (CPI): The program/project shall protect the confidentiality of command link CPI as NASA SBU information to prevent inadvertent disclosure to unauthorized parties per NASA NID 1600.55 and NPR 2810.1.

Ensure Positioning, Navigation, and Timing (PNT) Resilience

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

Report Unexplained Interference

- Interference Reporting: Projects/Spectrum Managers/Operations Centers shall report unexplained interference to MRPP or to other designated notifying organizations.
- Interference Reporting Training: Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.

https://standards.nasa.gov/standard/oce/nasa-std-1006-wchange-1