NOT MEASUREMENT SENSITIVE

NASA TECHNICAL STANDARD

NASA-STD-1006

Office of the NASA Chief Engineer

Approved: 2019-10-29

SPACE SYSTEM PROTECTION STANDARD

DOCUMENT HISTORY LOG

Status	Document Revision	Change Number	Approval Date	Description
Baseline			2019-10-29	Initial Release

FOREWORD

This NASA Technical Standard is published by the National Aeronautics and Space Administration (NASA) to provide uniform engineering and technical requirements for processes, procedures, practices, and methods that have been endorsed as standard for NASA programs and projects, including requirements for selection, application, and design criteria of an item.

This NASA Technical Standard is approved for use by NASA Headquarters and NASA Centers and Facilities, and applicable technical requirements may be cited in contract, program, and other Agency documents. It may also apply to the Jet Propulsion Laboratory (a Federally Funded Research and Development Center [FFRDC]), other contractors, recipients of grants and cooperative agreements, and parties to other agreements only to the extent specified or referenced in applicable contracts, grants, or agreements.

This NASA Technical Standard establishes Agency-level protection requirements to ensure NASA missions are resilient to threats and is applicable to all NASA programs and projects.

Requests for information should be submitted via "Feedback" at https://standards.nasa.gov. Requests for changes to this NASA Technical Standard should be submitted via MSFC Form 4657, Change Request for a NASA Engineering Standard.

Original signed by
Ralph R. Roe, Jr.
NASA Chief Engineer

2019-10-29
Approval Date

TABLE OF CONTENTS

LIST OF APPENDICES

SPACE SYSTEM PROTECTION STANDARD

1. SCOPE

1.1 Purpose

The purpose of this NASA Technical Standard is to establish Agency-level protection requirements to ensure NASA missions are resilient to purposeful threats.

1.2 Applicability

This NASA Technical Standard is applicable to all NASA programs and projects.

This NASA Technical Standard is approved for use by NASA Headquarters and NASA Centers and Facilities, and applicable technical requirements may be cited in contract, program, and other Agency documents. It may also apply to the Jet Propulsion Laboratory (a Federally Funded Research and Development Center [FFRDC]), other contractors, recipients of grants and cooperative agreements, and parties to other agreements only to the extent specified or referenced in applicable contracts, grants, or agreements.

Verifiable requirement statements are designated by the acronym “SSPR” (Space System Protection Requirement), numbered, and indicated by the word “shall”; this NASA Technical Standard contains six (6) requirements. To facilitate requirements selection by NASA programs and projects, a Requirements Compliance Matrix is provided in Appendix A. Programs and projects should document adoption of the requirements in their Project Protection Plan. Explanatory or guidance text is indicated in italics beginning in section 4.

1.3 Tailoring

Document tailoring of the requirements in this NASA Technical Standard for application to a specific program or project as part of program or project requirements in the Project Plan and obtain formal approval by the delegated Technical Authority or requirement owner in accordance with NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

2. APPLICABLE DOCUMENTS

2.1 General

The documents listed in this section contain provisions that constitute requirements of this NASA Technical Standard as cited in the text.

2.1.1 The latest issuances of cited documents apply unless specific versions are designated.

2.1.2 Non-use of a specifically designated version is approved by the delegated Technical Authority.

Applicable documents may be accessed at https://standards.nasa.gov, https://nodis3.gsfc.nasa.gov/, or obtained directly from the Standards Developing Body or other document distributors. When not available from these sources, information for obtaining the document is provided.

References are provided in Appendix B.

2.2 Government Documents

National Aeronautics and Space Administration (NASA)

NPR 2810.1	Security of Information Technology
NPR 7120.5	NASA Space Flight Program and Project Management Requirements
NID 1600.55	Sensitive But Unclassified (SBU) Controlled Information
FIPS 140	Security Requirements for Cryptographic Modules (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards)

2.3 Non-Government Documents

None.

2.4 Order of Precedence

2.4.1 The requirements and standard practices established in this NASA Technical Standard do not supersede or waive existing requirements and standard practices found in other Agency documentation, or in applicable laws and regulations unless a specific exemption has been obtained by the Office of the NASA Chief Engineer.

2.4.2 Conflicts between this NASA Technical Standard and other requirements documents are resolved by the delegated Technical Authority.

3. ACRONYMS, ABBREVIATIONS, AND DEFINITIONS

3.1 Acronyms and Abbreviations

CCSDS	Consultative Committee for Space Data Systems

CPI	Critical Program/Project Information
EOM	End of Mission
EPP	Enterprise Protection Program
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
MOC	Mission Operations Center
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NESC	NASA Engineering and Safety Center
NID	NASA Interim Standard
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
PNT	Positioning, Navigation, and Timing
RF	Radio Frequency
SAPP	Space Asset Protection Program
SBU	Sensitive But Unclassified
SOC	Science Operations Center
SSPR	Space System Protection Requirement
STD	Standard

3.2 Definitions

Command Link: Free space command path connection from transmission at the ground system terminal or space transmitter to receipt by the spacecraft receiver.

Command Stack: The end-to-end command chain from initial command transmission at the operations center to receipt and execution on the platform.

Critical Project Information: Sensitive information, which, if compromised, inappropriately disclosed, falsified, or made unavailable could enable an adversary to cause mission loss/degradation and/or damage to other space systems.

Deep Space: Space beyond 2 million kilometers from the Earth.

Hardware Commands: Spacecraft commands that, once extracted by the spacecraft hardware from the uplink command channel, are routed to a specific location and are executed on receipt, without any flight software interaction.

4. SPACE SYSTEM PROTECTION REQUIREMENTS

4.1 Maintain Command Authority

Objective: Missions need to maintain command authority to prevent unauthorized access and to ensure data integrity. Unauthorized access could result in mission loss and/or damage to other space systems.

4.1.1 Command Stack Protection

[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.

4.1.1.a *[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.]*

4.1.1.b *This requirement may be tailored to accommodate the nature of the mission. The following tailoring is suggested for use by applicable missions:*

i. Hosted instruments only require protection of the instrument command stack.
ii. Hosted instruments are only responsible for protection of the command stack until the host spacecraft operations center receives commands.
iii. Deep space missions may choose to limit controls applied to the space link if certain controls (e.g. encryption and authentication) pose significant burden to operability or mission success, and if the threat to the space link is low.
iv. Category 3/Class C or Class D missions may authenticate without encryption if they have no propulsion.

4.1.1.c *The following guidance is offered to assist missions in implementing this requirement:*

i. Missions should pursue multiple protections as a defense in-depth measure (e.g. encryption and authentication).
ii. Missions can select an appropriate encryption scheme for each leg of the command path, e.g. SOC->MOC->Station->Spacecraft.
iii. Crewed missions should also protect intra-vehicle and intra-suit communications.
iv. Missions should protect the integrity of the command generation process.
v. Missions using Consultative Committee for Space Data Systems (CCSDS) should consult CCSDS 350.0-G, The Application of Security to CCSDS Protocols, CCSDS 355.0-B, Space Data Link Security Protocol, and CCSDS 352.0-B, CCSDS Cryptographic Algorithms. Note that FIPS 140 compliance meets and exceeds the cryptographic specifications of CCSDS 352.0-B.

4.1.2 Backup Command Link Protection

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

4.1.2.a *[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)

[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.

4.1.3.a *[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.]*

4.1.3.b *The following guidance is offered to assist missions in implementing this requirement:*

i. The Space Asset Protection Program (SAPP) can assist the program/project with command link CPI identification.
ii. Command link CPI may include sensitive command information such as hardware commands, key handling/management, and bit patterns of critical commands.

4.2 Ensure Positioning, Navigation, and Timing (PNT) Resilience

Objective: Missions dependent on external PNT services need to be able to recognize and survive interference to ensure PNT resilience. Extended loss of PNT services could result in mission degradation or loss if no mitigations are available.

4.2.1 Positioning, Navigation, and Timing (PNT) Resilience

[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.

4.2.1.a *[Rationale: Per www.gps.gov, PNT systems are subject to interference from both natural and human-made sources.]*

4.2.1.b *The following guidance is offered to assist missions in performing trade studies to evaluate the risk and impact of a denial of PNT services and to design appropriate mitigations, as appropriate:*

i. *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, Navigation Filter Best Practices, describes NESC Best Practices for navigation filter design.*
ii. *PNT computations should be tested for resiliency to invalid parameter inputs, e.g. as specified in the current version of Global Positioning System (GPS) interface specification IS-GPS-200, Navstar GPS Space Segment/Navigation User.*
iii. *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.*
iv. *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 consideratons in their planning and possibly incorporate design features in the flight or ground hardware to provide for backup PNT capabilities.*
v. *Missions requiring PNT services should also consult NPD 8900.4, NASA Use of Global Positioning System Precise Positioning Service.*

4.3 Report Unexplained Interference

Objective: Missions need to detect and report instances of unexplained interference to enable Agency awareness of the contested space environment and to develop appropriate mitigations. Lack of Agency awareness of unexplained interference events could deprive NASA of indications and warning of adversary actions and increase the vulnerability of NASA systems.

4.3.1 Interference Reporting

[SSPR 5] Projects/Spectrum Managers/Operations Centers shall report unexplained interference to SAPP or to other designated notifying organizations.

4.3.1.a *[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.]*

4.3.1.b *The following guidance is offered to assist missions in implementing this requirement:*

i. *Hosted instruments need only monitor indigenous telemetry and mission data.*
ii. *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.*
iii. *Missions should incorporate procedures for operations teams to contact NASA SAPP 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.*
iv. *This requirement may be implemented in either the space segment or the ground segment.*
v. *In the absence of a designated notifying organization, contact NASA SAPP via gsfc-dl-sapp@mail.nasa.gov.*
vi. *SAPP, in coordination with the Enterprise Protection Program (EPP), will maintain a registery of NASA notifying organizations, responsibilities of notifying organizations, and external recipients of NASA notifications.*
vii. *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.)*

4.3.2 Interference Reporting Training

[SSPR 6] Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.

4.3.2.a *[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.]*

4.3.2.b *The following guidance is offered to assist missions in implementing this requirement: Missions should conduct training annually, as a minimum, using the latest reporting procedures.*

APPENDIX A

REQUIREMENTS COMPLIANCE MATRIX

A.1 Purpose/Scope

Due to the complexity and uniqueness of space flight, it is unlikely that all of the requirements in a NASA technical standard will apply. The Requirements Compliance Matrix below contains this NASA Technical Standard's technical authority requirements and may be used by programs and projects to indicate requirements that are applicable or not applicable to help minimize costs. Enter "Yes" in the "Applicable" column if the requirement is applicable to the program or project or "No" if the requirement is not applicable to the program or project. The "Comments" column may be used to provide specific instructions on how to apply the requirement or to specify proposed tailoring.

NASA-STD-1006				
Section	**Description**	**Requirement in this Standard**	**Applicable (Enter Yes or No)**	**Comments**
4.1.1	Command Stack Protection	[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.		
4.1.2	Backup Command Link Protection	[SSPR 2] If a project uses an encrypted primary command link, any backup command link shall, at a minimum, use authentication.		
4.1.3	Command Link Critical Program/Project Information (CPI)	[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.		
4.2.1	Positioning, Navigation, and Timing (PNT) Resilience	[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.		
4.3.1	Interference Reporting	[SSPR 5] Projects/Spectrum Managers/Operations Centers shall report unexplained interference to SAPP or to other designated notifying organizations.		

NASA-STD-1006				
Section	**Description**	**Requirement in this Standard**	**Applicable (Enter Yes or No)**	**Comments**
4.3.2	Interference Reporting Training	[SSPR 6] Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.		

APPENDIX B

REFERENCES

B.1 Purpose/Scope

This Appendix provides reference information to the user.

B.2 Reference Documents

	National Space Policy (https://www.space.commerce.gov/policy/national-space-policy/)
NPD 8900.4	NASA Use of Global Positioning System Precise Positioning Service
NPR 2570.1	NASA Radio Frequency (RF) Spectrum Management Manual
NASA/TP-2018-219822	Navigation Filter Best Practices
NIST Special Publication 800-160	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-160.pdf)
CCSDS 350.0-G	The Application of Security to CCSDS Protocols
CCSDS 352.0-B	CCSDS Cryptographic Algorithms
CCSDS 355.0-B	Space Data Link Security Protocol
IS-GPS-200	Global Positioning Systems Directorate, Systems Engineering and Integration, Interface Specification, Navstar GPS Space Segment/Navigation User Interfaces (https://www.gps.gov/)
MSFC Form 4657	Change Request for a NASA Engineering Standard