National Aeronautics and
Space Administration

SS BPG
REV A
RELEASE DATE: 18 OCT 2023

Space Security:
Best Practices Guide (BPG)

REVISION AND HISTORY

Revision No.	Change No.	Description	Release Date
-	N/A	Initial Release - Approved for Public Release	18 OCT 2023

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

1.1 PURPOSE

The Space Security: Best Practices Guide (BPG) provides guidance on mission security implementation in the form of principles coupled with applicable controls that cover both the space vehicle and the ground segment. The BPG leverages security controls as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and serves as a translation guide between NIST verbiage and NASA flight project parlance. The principles are meant to be easily achievable regardless of mission, program, or project size, scope, or whether international, corporate, or university. The principles selected focus on a risk-based approach to mitigating vulnerabilities, that are impediments to mission success. Principles were identified as an initial starting point of critical implementations for missions to consider. The underlying security principles and associated controls were identified through an iterative process to address today's cyber actors Tactics, Techniques, and Procedures (TTPs) used in attempts to compromise mission capabilities. The guide is to be used as an initial starting point to mitigate against any efforts to deny, degrade, disrupt, deceive, or destroy information and technology used to accomplish NASA mission success.

1.2 SCOPE

This guidance applies to all mission, programs, and projects regardless of class. Missions, programs, and projects are encouraged to use this document as a baseline for space security principles. While this document is still in guidance form, the principles and controls will be evaluated for inclusion into the main body of NASA Agency standards and requirements. It is important that the missions, programs, and projects provide feedback on utility and implementation of this guide to the Enterprise Protection Program (EPP) and Office of the Chief Information Officer (OCIO). The term "mission" is meant to be all encompassing and include all NASA missions, programs, and projects.

This Best Practices Guide provides guidance specific to mission, programs, and projects not already covered in the existing NPRs and Standards. This guide does not replace Agency requirement for missions to develop a System Security Plan (SSP) as identified in NPD 2800.1, NPR 2810, and NPR 7120.5. Figure 1 shows a mapping of the documents influencing the mission managers risk and programmatic decisions.

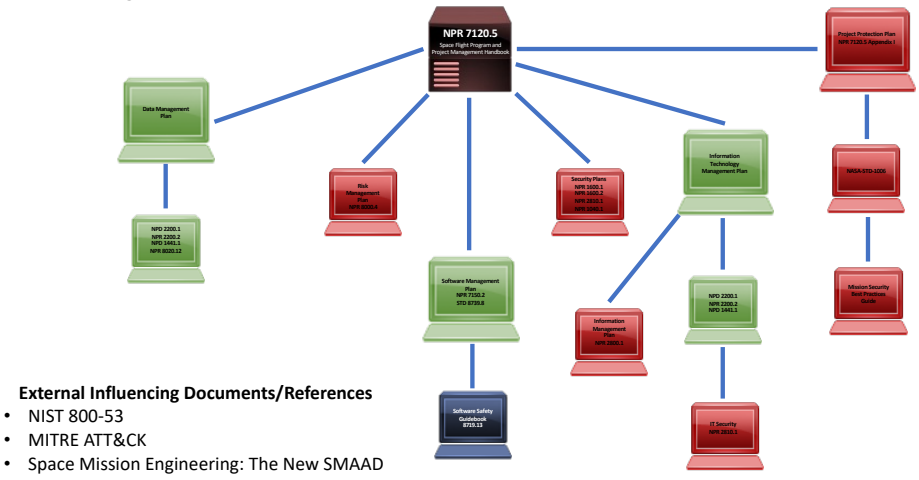

Figure 1 Documents Influencing the Mission Manager

Due to the significant architectural, developmental (lifecycle), and operational differences between the space mission and ground segments, this document sets forth principles in both space mission and ground segments. Readers are encouraged to view the full set of principles as designed to work together to provide a layered and comprehensive defense. In addition to the two segments, a single governance principle has been selected to provide context and guidance for mission executive and operational leadership to include cybersecurity risk considerations in budgeting and planning.

1.3 CHANGE AUTHORITY/RESPONSIBILITY

Currently, the Best Practice Guide will be issued under the auspices of the Enterprise Protection Program, in coordination with OCIO, and will gather feedback on the principles with the goals of incorporating the principles into an official NASA Standard. The standard will be developed along the lines of how NASA-STD-1006 was developed. It is expected to move this process through a more accelerated timeline to meet both the needs of the missions who are actively designing and developing their technical principles and the rapidly evolving capabilities of actors.

Proposed changes to this document shall be submitted via a Change Request (CR), found in Appendix F, to the Enterprise Protection Program for consideration and disposition. All such requests will be evaluated semi-annually (by a large group) for inclusion or exclusion in future versions of the guide. If a principle is recommended for implementation into a NASA STD/NPR/NPD or other document, it will be evaluated during the same semi-annual process.

1.4 CONVENTION AND NOTATION

The Enterprise Protection Program and Office of the Chief Information Officer defines its implementation of principle verb as follows:

“Should” – Used to indicate good practice or a goal which is desirable but not mandatory and does not require formal verification. As applied to payloads, requirements identified to specify proper hardware and software interfaces to contribute to overall payload mission success are specified with “should” statements. “Should” statements not followed could result in operational constraints or failure to meet payload objectives.

Rationales for many of the principles are intended to provide clarification, justification, purpose, or the source of a principle. In the event that there is an inconsistency between a principle and its rationale, the principle always takes precedence.

1.4.1 Principle Identification

The controls listed in this Best Practices Guide use a naming schema consisting of three parts. The first section identifies where the principle is applied, either mission, ground, or governance. The second section identifies the portion of the system the principle is applied. The final section is a sequential number for the principle.

1.4.2 Information Included with the Principles

In addition to the principle language and rationale, there are four additional pieces of information (controls):

- Aerospace Space Threat Actor Capabilities
- MITRE ATT&K Threat Actor Tactics
- NIST 800-53 Revision 5 applicable cybersecurity controls
- Space Mission Security and Protection Key Performance Parameters

There are seven Threat Actor Capabilities that are tied to the original Aerospace Technical Operating Report (Aerospace TOR-2021-01333), where multiple capabilities may be invoked by the cyber actor:

- CAP-01: Ability to Access Networks
- CAP-02: Ability to Discover and Exploit Vulnerabilities
- CAP-03: Ability to Defeat Cryptography and Authentication
- CAP-04: Command and Control Sophistication
- CAP-05: Ability to Affect Cyber and/or Physical Systems
- CAP-06: Ability to Gain Physical Access
- CAP-07: Sophistication of Human Influence

Additionally, the MITRE ATT&K Threat Actor Tactics (https://attack.mitre.org/) were explored to provide the reader with potential paths for mitigations. There are twelve tactics that were introduced from Industrial Control Systems (ICS) or Operational Technologies (OT). Why would one use ICS or OT tactics vs traditional cybersecurity tactics on a space mission system? ICS and OT systems have very similar requirements to space mission systems for timing and are often networked together. Space-based mission systems often have multiple operating systems on a variety of processors, that are often not protected (except the command link). Further since Government and commercially developed spacecraft are currently incorporating common standards and architectures such as TCP/IP and UDP in their design to enable systems interconnection and communication. Additionally, incorporation of newer technology such as artificial intelligence (AI) and machine language (ML) applications will potentially expand the protection needs. As the integration and interconnection of systems continues to occur in the future, it is important to consider the spacecraft from both information system and operational technology views. The protection of increasingly more complex space systems will necessitate the adaptation and implementation of Best Practices as they relate to design, intended operations, interconnections, and zero trust perspectives. The MITRE ATT&CK Threat Actor Tactics used were:

- TAC-01: Initial Access
- TAC-02: Execution
- TAC-03: Persistence
- TAC-04: Privilege Escalation
- TAC-05: Evasion
- TAC-06: Discovery
- TAC-07: Lateral Movement
- TAC-08: Collection
- TAC-09: Command and Control
- TAC-10: Inhibit Response Function
- TAC-11: Impair Process Control
- TAC-12: Impact

Lastly the Space Mission Security and Protection Key Performance Parameters were used to round out the risk-based approach. These key performance parameters are divided into three areas or pillars to ensure a space mission systems survivability/resiliency:

- PREVENT: Design principles that remove the likelihood of cyber events
- MITIGATE: Design principles that reduce the impact and/or likelihood of cyber events
- RECOVER: Design principles that enable resiliency and restoration of capabilities impaired due to a cyber event

Because there is no risk management framework for end-to-end integrated space mission systems the combination of these four practices provides the beginnings of an informed risk management framework for space missions. This combination will eventually enable engineers, program managers, and leaders to make informed risk management decisions for space mission cybersecurity and protection based in a system similar to what already exists for other risk decisions that is comfortable and known. This system will be developed in the second release of the guide.

1.5 BACKGROUND

During the months of October through December of 2021, team members from Enterprise Protection Program (EPP) and the Office of the Chief Information Officer (OCIO) worked to generate awareness of the need for clearly defined guidance for space mission and ground segment cybersecurity controls. This process, driven by an explicit goal to develop a consensus approach, met with stakeholders from across the Agency to solicit input and request participation in a future working group.

Upon approval from the Enterprise Protection Board (EPB) to explore this topic further, EPP and OCIO kicked-off the “Spacecraft Cyber Controls Working Group” with 45 key stakeholders from OCIO, OCE, OSMA, SOMD, ESDMD, STMD, JPL, and SMD. The working group leveraged existing research, reference material, and work already completed as noted below:

- Risk analysis, vulnerability mapping, and critical cyber controls for Space Vehicle and Ground segments completed by Aerospace Corporation
- Flight Operations Directorate and Mission Control Center evaluation of operational environment, contracts, and associated cybersecurity controls
- Cybersecurity requirements guidance and control template already completed by Gateway

Through numerous feedback sessions and draft revisions with key stakeholders, a final set of 27 controls was finalized for the Space Security: Best Practices Guide (BPG).

The final document was formatted and sent out for approval October 2023.

1.6 FREQUENTLY ASKED QUESTIONS

There were many questions that were asked during the Best Practices Guide creation. What follows are the most frequently asked:

- Why a Best Practices Guide versus formal technical requirements?
    - After surveying available options for release of this artifact to NASA’s mission community, it was determined by the community that a Best Practices Guide would allow for timely and streamlined release

  - Formal technical requirements, similar to those existing in NASA-STD-1006, can take significant time to adopt in the mission community; due to the dynamic nature of the space mission cybersecurity and protection area a more robust process will need to be defined and undertaken; we may ultimately adopt some portion of this document into formal technical standards
  - The practices here do not have immediate solutions in all mission types and architectures, and formal requirements may not be achievable or cost effective for many missions until these concepts are implemented in product lines
- There are two distinct categories of space security principles: space mission and ground segment. What were the original sources for each group of principles?
  - Space Mission
    - The starting point for space mission critical principles was the risk and vulnerability landscape applicable to space vehicle and reflects a risk-based approach for the selection of controls; space vehicle risk analysis research was leveraged that was conducted by Aerospace Corporation, vetted by Department of Defense (DOD) space subject matter experts, and approved for release by DOD
  - Ground Segment
    - For the ground segment, analysis was leveraged that was completed by FOD/MCC in which NIST 800-53 controls applicable to the ground segment were utilized and created a prioritization framework based on five criteria: positioning and control, monitoring, availability, integrity, and confidentiality
    - Work done by Aerospace Corporation for ground segment was also utilized, which provided categorization of the NIST 800-53 controls based on a set of questions aimed at mission teams
  - For both the space mission and ground segments, the principles were down-selected and aggregated to reach a preliminary set of Best Practice Guide critical principles based on the above analysis and an orthogonal review to ensure the principles proposed were sufficient to address the various stages of known cyber actors techniques as developed in MITRE's ATT&CK framework
  - Due to NASA's civil nature specific tuning of the principles and controls were necessary to ensure there was not excessive language or overly restrictive principles placed on missions, programs, and projects
- Is selection of these principles tied in any way to a system security categorization such as per FIPS 199? Or are these principles intended to be applied in a risk appropriate manner to all spacecraft and ground segments?
  - While these Best Practices Guide principles will be mapped to NIST 800-53 controls, and therefore can guide the development of a System Security Plan (SSP) designed to support the Authority to Operate (ATO) process for systems at each of the FIPS 199 categories (LOW, MODERATE, HIGH), Best Practices Guide principle selection was based on risk modelling and should be used to prioritize principles from a defense in depth model

2. DOCUMENTS

2.1 APPLICABLE DOCUMENTS

Document Number	Revision	Document Title
ATT&CK	October 2022	MITRE ATT&CK
CJCSI 6510.01	June 2015	Information Assurance (IA) and Support to Computer Network Defense (CND)
DODI 8110.01	June 2021	Mission Partner Environment Information Sharing Capability Implementation for the DoD
DODI 8500.01	October 2019	Cybersecurity
GP 10037	July 2021	Gateway Payload Interface Definition Document
GSFC-STD-1000	June 2016	Goddard Space Flight Center Rules for the Design, Development, Verification, and Operation of Flight Systems
NASA-GB-8719.13	March 2004	NASA Software Safety Guidebook
NASA-STD-1006	November 2020	Space System Protection Standard
NASA-STD-8739.8	September 2022	Software Assurance and Software Safety
NIST 800-53	September 2020	Security and Privacy Controls for Information Systems and Organizations
NPD 2200.1	January 2020	Management of NASA Scientific and Technical Information
NPD 2800.1	December 2019	Managing Information Technology
NPR 1040.1	July 2003	NASA Continuity of Operations (COOP) Planning Procedural Requirements
NPR 1441.1	January 2015	NASA Records Management Program Requirements
NPR 1600.1	August 2013	NASA Security Program Procedural Requirements
NPR 1600.2	September 2019	NASA Classified National Security Information
NPR 2200.2	December 2021	Requirements for Documentation, Approval and Dissemination of Scientific and Technical Information
NPR 2810.1	January 2022	Security of Information and Information Systems
NPR 7120.5	August 2021	NASA Space Flight Program and Project Management Requirements w/Change 1

Document Number	Revision	Document Title
NPR 7120.7	August 2020	NASA Information Technology Program and Project Management Requirements
NPR 7120.8	September 2018	NASA Research and Technology Program and Project Management Requirements (Updated w/Chage 2)
NPR 7123.1	February 2020	NASA Systems Engineering Processes and Requirements (w/Change 2)
NPR 7150.2	March 2022	NASA Software Engineering Requirements
NPR 8000.4	April 2022	Agency Risk Management Procedural Requirements
TOR-2018-02275	August 2018	A Need for Robust Space Vehicle Cybersecurity
TOR-2019-02178	August 2019	Satellite Telemetry Indicators for Identifying Potential Cyber Attacks
TOR-2021-01333	April 2021	Cybersecurity Protections for Spacecraft: A Threat Based Approach
TOR-2021-01725	June 2021	Cybersecurity Protections for Space Systems

2.2 ORDER OF PRECEDENCE

In the event of a conflict between the principles and controls of this document and references used to create, the principles of this document are best practices and are not to supersede referenced documentation. Resolution of any precedence conflicts are accomplished through the use of waivers and deviations, or as per discretion of the mission manager. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. MISSION SECURITY

3.1 GOVERNANCE

3.1.1 Governance Background

Governance principles and controls address overarching mission, program, project themes that should be addressed within the mission, program, project.

3.1.2 Principles and Associated Controls for Governance

This section provides the individual principles and associated controls related to Governance.

3.1.2.1 GV-RSK-01 Adaptive Risk Response and Resource Allocation Function

Principle: *As a best practice the mission should establish a continuous process of qualitative and quantitative mission security risk analysis and risk response for the duration of the mission.*

As a best practice the mission should establish a continuous process of qualitative and quantitative mission security risk analysis and risk response for the duration of the mission.

Rationale: Static cybersecurity defenses are not sufficient to rapidly adapt to changing risk conditions such as the discovery of a new cyber actors modular attack toolkit with the capability to integrate targeting packages for entirely new platforms in very short time frames. This requirement calls for the design and operationalization of an organizational model for cybersecurity defense that can rapidly integrate new information across the entire lifecycle and toolkit to reconfigure how architecture, design, testing, deployment, patching, monitoring, analytics, alerting, and response activities are triggered, focused, and automated.

Risk mitigation recommendations should include, but not be limited to, making risk-appropriate budgeting, contracting, procurement, and personnel assignment decisions. Effectively acting to mitigate the identified risks will require support from the mission's management chain and mission support providers.

This Principle Addresses These Controls:

- Addresses All CAP
- Addresses All TAC
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) PM-9, PM-28, RA-7
- Addresses ALL Space Mission Security and Protection Pillars

3.2 SPACE MISSION

3.2.1 Space Mission Background

Space mission principles will be principles that are applicable to the space vehicle, space-based hosted payload, or space-based infrastructure or architecture.

3.2.2 Principles and Associated Controls for Space Missions

This section provides the individual principles and associated controls related to Space Missions.

3.2.2.1 Architecture

3.2.2.1.1 MI-ARCH-01 Mission Essential Data Flow Function

Principle: *The mission should establish and maintain a current and accurate data flow diagram covering mission essential data flows, including those that pass through mission-external service providers.*

Rationale: A good data flow diagram provides understanding what data is needed by the system, and how that data flows across networks and communications links. In turn, this provides essential insight to understand where particular risk to the system may emerge, and where additional scrutiny or defenses may be warranted.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactic: TAC-02: Execution

- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-4, AC-4(2), AC-4(3), AC-4(6), AC-4(21), CA-3, CA-3(6), SC-32
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.2.2.1.2 MI-ARCH-02 Mission Least Privilege Function

Principle: *The mission should employ the principles of domain separation and least privilege for the on-board architecture, communications, and control.*

Rationale: Least privilege designs will protect the main processor and core control functions of the vehicle from compromised assemblies by limiting the actions that can be executed on shared buses and onboard networks from recognized attack vectors. Segmentation and boundary control on the vehicle will mitigate supply chain attacks in procured or provided assemblies and in onboard software of varying provenance, as well as operational vulnerabilities when multiple command paths are available (e.g., an instrument with its own command link). Fault management systems should be employed to power off or block non-safety-critical assemblies that exhibit behavior that suggests compromise or failure.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-01: Ability to Access Networks
- Interdicts Earliest Threat Actor Tactic: TAC-07: Lateral Movement
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-3, AC-4, AC-6, SA-8(14), SA-17(7), SC-3, SC-4, SC-6, SC-7(20), SC-7(21), SC-39, SI-17
- Addresses PREVENT Space Mission Security and Protection Pillar

3.2.2.2 Authentication and Authorization

3.2.2.2.1 MI-AUTH-01 Boundary Protection Function

Principle: *The mission should establish a mediated access mechanism that prevents unauthorized access to critical subsystems in the space segment.*

Rationale: Cyber actors can exploit the ground system and use the ground segment to maliciously interact with the space vehicle. The boundary protection may be logical or physical. Functionality provides the following benefits:

- Blocks unintended (incoming/outgoing) traffic
- Enables generation and maintenance of Security Logs
- Prevents devices from polling other network devices
- Prevents devices from polling the network for other devices
- Prevents bridging of networks

Effective boundary protection should/would include confidentiality protection using encryption (as defined by NASA STD 1006) in addition to some form of authentication (e.g., Galois/Counter Mode GCM). This boundary protection also needs to include protection on the space vehicle side where it protects itself from the ground being used as an attack vector. The inherent trust between the ground and space vehicle needs addressed where the space vehicle can protect itself from the ground in the event the ground has been compromised. Each mission should identify/define their most critical subsystems. Critical subsystems or control interfaces should have mediated access between mission critical control interfaces, that could create mission ending failure/consequence through either physical or software means.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-01: Ability to Access Networks
- Interdicts Earliest Threat Actor Tactic: TAC-12: Impact
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(9), SC-7(10), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(15), SC-7(16), SC-7(17), SC-7(18), SC-7(19), SC-7(20), SC-7(21), SC-7(22), SC-7(28), SC-7(29)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.2.2.2.2 MI-AUTH-02 Comprehensive Authentication and Authorization Function

Principle: *The mission should ensure only authenticated and authorized personnel, devices, and software are allowed to access the space mission system.*

Rationale:

- Cyber actors can masquerade as an authorized entity in order to gain access.
- Unique identifiers and associated authenticators (passwords, multi-factor physical and virtual, securely registered biometrics) and associated processes to verify entities at time of issuance and authenticate entities at time of access request allow the mission to provide a risk-aligned level of assurance that only vetted entities are allowed to access mission digital resources.
- Non-mission users authorized to access mission computing resources as a specific subset of all personnel pose a potential additional risk compared to mission users due to limited ability to fully vet and verify their suitability. Therefore, the mission should perform a risk assessment to determine the authorization needs of non-mission users that need to access the system (e.g., public users supporting commercial organizations); what information they would need to access; and its restrictions (OPSEC, Privacy Act, ITAR, etc.). The risk assessment should incorporate supply chain considerations related to foreign national access to Agency or other potentially sensitive information.
- The existence of insecure static authenticators for access to applications and control systems, such as hardcoded plaintext passwords or access tokens, can be discovered by cyber actors, brute forced, and reused across multiple similar systems creating an opportunity for rapid widespread compromise within the mission ground segment. Therefore, the mission should define policy and procedures to ensure that the developed or delivered systems do not embed unencrypted static authenticators in applications, access scripts, configuration files, or store unencrypted static authenticators on function keys. With associated decryptors on the space mission system.
- Ensuring only devices known to and registered with the appropriate mission device inventory and management platforms are allowed to access mission communications networks significantly reduces the increased risk due to unknown devices operating within mission environments. Therefore, the mission should provide the capability to uniquely identify and authenticate all types of computing devices, including mobile devices and network connected endpoint devices (including workstations, printers, servers, VoIP Phones, VTC CODECs) before establishing a network connection. In addition, the mission should, in consultation with the system security engineers and the AO, select the appropriate device identification and authentication mechanisms based on mission needs and the strength of mechanism required in support of that mission. Ensuring on the space mission system the right system has sent the right command at the right time.
- The mission should establish policy and procedures to prevent individuals (i.e., insiders) from masquerading as individuals with valid access to areas where commanding/updating

of the space vehicle is possible. mission must ensure a comprehensive authentication and authorization function (i.e., COMSEC and strong authentication) is available to prevent attacker from performing potential mission ending actions like flight software upgrades, burning read-only memory, changing fault responses, uploading stored command sequences, or executing mission defined critical commands. The equipment and protocols being used should include stronger encryption, authentication, and key management procedures to reduce risk of confidentiality and integrity violations and impacting the mission.

- While the rationale for this control appears to be more ground centric, while the space mission system is in development mission personnel will be requiring access outlined in the control.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities:
  - CAP-01: Ability to Access Networks
  - CAP-02: Ability to Discover and Exploit Vulnerabilities
  - CAP-05: Ability to Affect Cyber/Physical Systems
  - CAP-07: Sophistication of Human Influence
- Interdicts Earliest Threat Actor Tactics:
  - TAC-01: Initial Access
  - TAC-02: Execution
  - TAC-04: Privilege Escalation
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PE-3, PM-10, SI-7(15)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.2.2.3 Defensive Cybersecurity Operation

3.2.2.3.1 MI-DCO-01 Mission Cyber Actor Actions Detection Function

Principle: *The mission should incorporate an on-board cyber actor actions detection function in its requirements and resulting system.*

Rationale: The mission should plan for the possibility of an on-board disruption deriving from a security incident and incorporate these considerations. Event detection, mitigations, and alerting of ground segment security operations team are critical controls to provide the capability for operational teams to know when other controls have failed, rapidly respond (where possible). The resulting lessons learned should be fed back into the design process. Monitoring of key software observables (e.g., number of failed login attempts, unscheduled lockups of the flight receiver, indications of RFI on non-telecom equipment, performance changes, internal communication changes) is needed to detect cyber actor actions that interdict mission success.

Cybersecurity attacks affecting components of in-flight systems are expected. A cybersecurity incident response plan is key to the timely and effective response to a cybersecurity attack. All suspected cyber actor actions should be reported. Raw event data should be further analyzed to determine whether an anomalous event represents an attack, and if so, the nature of the attack, and the appropriate response to mitigate impact to the mission. Ensure the mission is following NPR 7150.2 guidance for software to detect cyber actor actions, such as those in 3.11.8.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-04: Command and Control Sophistication
- Interdicts Earliest Threat Actor Tactic: TAC-01: Initial Access
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-4(15), AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-14, CM-8(3), RA-5(7), SC-5(3), SC-7(9), SI-3(8), SI-4(1), SI-4(2), SI-4(4), SI-4(10), SI-4(11), SI-4(12), SI-4(13), SI-4(14), SI-4(15), SI-4(16), SI-4(17), SI-4(18), SI-4(19), SI-4(20), SI-4(22), SI-4(23), SI-4(24)
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.2.2.3.2 MI-DCO-02 Mission Fault Management Function

Principle: *The mission should incorporate fault management bypass protection in its requirements and resulting system.*

Rationale: The mission should consider the possibility of fault management transitions to bypass the system's protection measures and incorporate these considerations. Fault management systems may be deliberately triggered in an effort to bypass the system's protective measures. For example, safehold mode operations without command-link protection.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-04: Command and Control Sophistication
- Interdicts Earliest Threat Actor Tactic: TAC-01: Initial Access
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-4(15), AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-14, CM-8(3), RA-5(7), SC-5(3), SC-7(9), SI-3(8), SI-4(1), SI-4(2), SI-4(4), SI-4(10), SI-4(11), SI-4(12), SI-4(13), SI-4(14), SI-4(15), SI-4(16), SI-4(17), SI-4(18), SI-4(19), SI-4(20), SI-4(22), SI-4(23), SI-4(24)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.2.2.4 Integrity

3.2.2.4.1 MI-INTG-01 Communications Survivability Function

Principle: *The mission should be able to recover from communications jamming and spoofing attempts.*

Rationale: Communications systems using a shared medium are susceptible to jamming and spoofing, resulting in loss of access (denial of service) and potential loss of data integrity and availability. The prevalence of impacts to communications links in the RF and optical bands is increasing, as well as potential for targeted spoofing of communications links.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-05: Ability to Affect Cyber/Physical Systems
- Interdicts Earliest Threat Actor Tactic: TAC-10: Inhibit Response Function
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CP-8, SC-5, SC-8, SC-40, SC-40(1), SC-40(3), SI-10(3), SI-10(5), SI-10(6)
- Addresses RECOVER Space Mission Security and Protection Pillar

3.2.2.4.2 MI-INTG-02 Positioning, Navigation, and Timing Survivability Function

Principle: *The mission should be able to recover from positioning, navigation, and timing jamming and spoofing attempts.*

Rationale: As a specific example of MI-INTG-01, space-based Positioning, Navigation, and Timing (PNT) relying on a GNSS signal may experience loss of signal (denial of service) and potential loss of the signal's data integrity. Manipulations (spoofing) of GNSS signal data may result in consequences to the space vehicles PNT.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-05: Ability to Affect Cyber/Physical Systems
- Interdicts Earliest Threat Actor Tactic: TAC-10: Inhibit Response Function
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AU-8, CP-8, SC-5, SC-40, SC-40(1), SC-40(3), SI-10(3), SI-10(4), SI-10(5), SI-10(6)
- Addresses RECOVER Space Mission Security and Protection Pillar

3.2.2.5 Mission Assurance

3.2.2.5.1 MI-MA-01 Mission Recovery Function

Principle: *The mission should include intentional disruptions consistent with the mission vulnerability analysis in anomaly detection, response, and recovery plans and designs in the flight segment and ground segment.*

Rationale: A complete defense-in-depth architecture includes the ability of the space vehicle to maintain safe operation through a security incident affecting flight or ground systems, and to recover to a nominal state once the incident is resolved. Security incidents should be considered alongside equipment failures, environmental events, natural disasters, and other sources of disruption in onboard fault handling, anomaly response, and continuity-of-operations planning to ensure mission resilience.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-05: Ability to Affect Cyber/Physical Systems
- Interdicts Earliest Threat Actor Tactic: TAC-10: Inhibit Response Function
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CP-2(5), IR-4, SA-8(24)
- Addresses RECOVER Space Mission Security and Protection Pillar

3.2.2.5.2 MI-MA-02 Cybersecurity-Safe State Function

Principle: *The mission should design secure vehicle fault management functions and safe mode operations.*

Rationale: Fault management systems are one of the targets a cyber actor will attempt to compromise. Designing security into these systems at the earliest opportunity is paramount. Security should also be considered as a potential root cause of system malfunction that is captured by the fault management system, and fault responses should be designed to mitigate security events alongside other causes of system failure.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactic: TAC-11: Impair Process Control
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CP-12, SI-17, IR-4(3), IR-4(5)
- Addresses RECOVER Space Mission Security and Protection Pillar

3.2.2.6 Malware Protection

3.2.2.6.1 MI-MALW-01 Mission Malware Protection Function

Principle: *The mission system software updates should be validated as free from malware prior to deployment, launch, and at defined regular intervals while the mission is in operations.*

Rationale: On-orbit software updates/upgrades/patches and all software updates should be checked for malware prior to load. Additionally, malware injected into space vehicle software modules via supply chain attack may not be discovered until well into flight and may be activated as a step in compromising a vehicle. Modules that have not been updated during flight may therefore still pose a risk. Regular scans on stored copies of flight modules using updated signatures may discover malware that has been in hiding, and regular monitoring of malware and vulnerability reports will also prompt response.

Integrity of software should be verified by employing a cryptographically secure hashing algorithm to determine the hash (digest value) of the system (or software update package) being evaluated. Additionally, the authenticity of the "control" or "reference" hash value, to which the system's hash is being compared, should also be signed using the private key of a cryptographic digital signature to ensure that the control value was supplied by a legitimate, trusted entity. The reason for this extra measure is that, in its absence, an attacker could modify the system being checked for integrity and also make a corresponding modification to the control hash value so that the subsequent integrity check still passes. This control aims to ensure that only legitimate entities can supply control hash values for software and update packages.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-05: Ability to Affect Cyber/Physical Systems
- Interdicts Earliest Threat Actor Tactic: TAC-02: Execution
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CM-4(1), CM-7(8), CM-14, RA-5, SA-10(1), SA-10(3), SA-10(4), SA-10(5), SA-10(6), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9), SI-2, SI-3, SI-21
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.2.2.6.2 MI-MALW-02 Mission Software, Programmable Logic Devices, and Firmware Integrity Function

Principle: *The mission should establish and verify the integrity of it's software images.*

Rationale: On-orbit software updates/upgrades/patches. If TT&C is compromised or MOC or even the developer's environment, the risk exists to do a variation of a supply chain attack where after

it is in orbit you inject malicious code or direct writes to memory. New or modified virus or malware will not be identified without updated manufacturer definitions. Blocks, removes, or recommends patches of commonly known virus or malware used to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Virus and malware includes: computer worms, trojan horses, ransomware, spyware, etc.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-05: Ability to Affect Cyber/Physical Systems Interdicts Earliest Threat Actor Tactic: TAC-02: Execution
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CM-4(1), CM-7(8), CM-14, RA-5, SA-10(1), SA-10(3), SA-10(4), SA-10(5), SA-10(6), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9), SI-2, SI-3, SI-7
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.2.2.7 Software Supply Chain Restriction

3.2.2.7.1 MI-SOFT-01 Software Mission Assurance Function

Principle: *The mission should perform software assurance via established procedures and technical methods.*

Rationale: The intent of this control is to ensure the provider follows a formal software development process when creating safety-critical software, including all MOTS, GOTS, COTS, open-source, library acquired, and reused software. Software assurance methods must extend into the development environment as well. In order to secure the development environment, the first step is understanding all the devices and people who interact with it. Maintain an accurate inventory of all people and assets that touch the development environment. Ensure strong multi-factor authentication is used across the development environment, especially for code repositories, as cyber actors may attempt to sneak malicious code into software that's being built without being detected. Use zero-trust access controls to the code repositories where possible. For example, ensure the main branches in repositories are protected from injecting malicious code. A secure development environment requires change management, privilege management, auditing, and in-depth monitoring across the environment. The objectives of the software assurance and software safety activities include the following:

- Ensuring that the processes, procedures, and products used to produce and sustain the software conform to all specified requirements and standards that govern those processes, procedures, and products
    - A set of activities that assess adherence to, and the adequacy of the software processes used to develop and modify software products
    - A set of activities that define and assess the adequacy of software processes to provide evidence that establishes confidence that the software processes are appropriate for and produce software products of suitable quality for their intended purposes
- Determining the degree of software quality obtained by the software products
- Ensuring that the software systems are safe and that the software safety-critical requirements are followed
- Ensuring that the software systems are secure

- Employing rigorous analysis and testing methodologies to identify objective evidence and conclusions to provide an independent assessment of critical products and processes throughout the lifecycle

The software development process should include software requirements definition, design, implementation, verification, maintenance, and retirement phases, and incorporate software quality assurance, configuration management, problem reporting and corrective action, reliability, maintainability, safety, verification and validation, certification, and operational use of the software. Additionally, software reuse, commercial off the shelf dependence, and standardization of onboard systems using building block approach with addition of open-source technology leads to a potential supply chain vulnerability that must be mitigated appropriately. See NPR 7150.2D, NASA Software Engineering Requirements and NASA-STD-8739.8B, Software Assurance and Software Safety Standard. Lastly, the mission should perform software assurance via established procedures and technical methods, including checking against NASA's Assessed and Cleared List.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactic: TAC-02: Execution
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CA-8, CM-3(2), CM-3(7), CM-3(8), CM-4, CM-5, CM-7(4), CM-7(5), CM-10, IR-4(10), IR-6(3), MA-3(6), PM-30, PM-30(1), RA-3(1), SA-4(3), SA-10(1), SA-15, SA-15(5), SA-15(7), SA-15(8), SA-15(11), SA-17, SA-20, SA-21, SI-2, SI-7, SR-1, SR-2, SR-3, SR-3(2), SR-3(3), SR-4(4), SR-7, SR-9
- Addresses PREVENT Space Mission Security and Protection Pillar

3.2.2.7.2 MI-SOFT-02 Software and Hardware Testing Function

Principle: *The mission should establish procedures and technical methods to perform end to end testing to include negative testing (i.e., abuse cases) of the mission hardware and software as it would be in an operating state (test as you fly).*

Rationale: Negative testing and analysis are necessary to validate that the system architecture and security-focused design features provide adequate resilience against a range of potential attacks. Where faulted testing is standard practice in the mission lifecycle, security cases should be added to the set of potential anomalous scenarios to test. Operational anomaly response training should include security events and exercise operational interfaces to institutional security organizations.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactic: TAC-02: Execution
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CA-8, CM-3(2), RA-5, RA-5(2), RA-5(3), SA-3, SA-4(3), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9)
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.3 GROUND

3.3.1 Ground Background

Ground principles will be principles that are applicable to the ground infrastructure, laboratory environment, or integrated ground architecture.

3.3.2 Principles and Associated Controls for Ground

This section provides the individual principles and associated controls related to the ground. NASA's ground systems are required be NPD/NPR 2810 to follow the NIST Risk Management Framework and the controls as described by the ITS-Handbooks and policy. The common controls and best practices below do not conflict with existing requirements, but they support the existing ATO process as defined by NPD/NPR 2810.

3.3.2.1 Authentication and Authorization

3.3.2.1.1 GR-AUTH-01 Unique Identifiers for Authentication Function

Principle: *The mission should provide the capability for each system to uniquely identify and authenticate organizational users and computing processes acting on behalf of organizational users.*

Rationale: The mission should manage authenticators used to access information system resources by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, device, or process (application, API, microservice) receiving the authenticator. Unique identifiers and associated authenticators (passwords, multi-factor physical and virtual, securely registered biometrics) and associated processes to verify entities at time of issuance and authenticate entities at time of access request allow the mission to provide a risk-aligned level of assurance that only vetted entities are allowed to access mission digital resources.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities:
  - CAP-01: Ability to Access Networks
  - CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactics:
  - TAC-01: Initial Access
  - TAC-02: Execution
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) IA-2(5), IA-2(8), IA-5
- Addresses PREVENT Space Mission Security and Protection Pillar

3.3.2.1.2 GR-AUTH-02 Risk-informed Authorization for Non-Mission Users Function

Principle: *The mission should use only verified identities when provisioning authenticators to organizational users and processes acting on behalf of users.*

Rationale: Mission users authorized to access mission computing resources pose a potential additional risk compared to Agency mission users due to limited ability to fully vet and verify their suitability.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-05: Ability to Affect Cyber/Physical Systems
- Interdicts Earliest Threat Actor Tactic: TAC-04: Privilege Escalation
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) IA-4(4), IA-8, IA-10, PM-10, PS-2, SI-4(19)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.3.2.1.3 GR-AUTH-03 Secure Workload-to-Workload Authenticator Function

Principle: *The mission should define policy and procedures to ensure that the developed or delivered systems do not embed unencrypted static authenticators in applications, access scripts, configuration files, nor store unencrypted static authenticators on function keys.*

Rationale: The existence of insecure static authenticators, such as hardcoded plaintext passwords or access tokens, can be discovered by cyber actors, brute forced, and reused across multiple similar systems creating an opportunity for rapid widespread compromise within the mission ground segment.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-01: Ability to Access Networks
- Interdicts Earliest Threat Actor Tactic: TAC-01: Initial Access
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) IA-5(7)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.3.2.2 Device Authentication

3.3.2.2.1 GR-DEVA-01 Computing Device Authentication Function

Principle: *The mission should provide the capability to uniquely identify and authenticate all types of computing devices, including mobile devices and network connected endpoint devices (including workstations, printers, servers, VoIP Phones, VTC CODECs) before establishing a network connection.*

Rationale: The mission should, in consultation with the system security engineers and the AO, select the appropriate device identification and authentication mechanisms based on mission needs and the strength of mechanism required in support of that mission.
Ensuring only devices known to and registered with the appropriate mission device inventory and management platforms are allowed to access mission communications networks and are regularly revalidated significantly reduces the increased risk due to unknown devices operating within mission environments.

The mission should ensure that the inventory of information system components includes minimally but not limited to: hardware specifications (manufacturer, type, model, serial number, physical location), software and software license information, information system/component owner, and for a networked component/device, the machine name.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities: CAP-01: Ability to Access Networks

- Interdicts Earliest Threat Actor Tactics: TAC-01: Initial Access
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) IA-3, IA-3(1), CM-8
- Addresses PREVENT Space Mission Security and Protection Pillar

3.3.2.3 Integrity

3.3.2.3.1 GR-INTG-01 Software and Firmware Integrity Verification Function

Principle:

- *The mission should require developers of information systems, system components, or information system services to enable integrity verification of software and firmware components prior to delivery and during mission operations*
- *Each system operated by the mission should provide the capability to verify the integrity of mission-defined software, firmware, and information*
- *The mission should provide and employ integrity verification tools to detect unauthorized changes to mission-defined software, firmware, and information*
- *The mission should define processes and procedures to be followed when integrity verification tools detect unauthorized changes to mission-defined software, firmware, and information*

Rationale: Cyber actors have adopted and are refining their capability to infiltrate software supply chains and to modify or replace valid software and firmware with compromised versions. Integrity verification via methods such as checking published hashes and proper validation of code signing certificates are important capabilities for mitigation of these attacker tactics.

Integrity of software should be verified by employing a cryptographically secure hashing algorithm to determine the hash (digest value) of the system (or software update package) being evaluated. Additionally, the authenticity of the "control" or "reference" hash value, to which the system's hash is being compared, should also be signed using the private key of a cryptographic digital signature to ensure that the control value was supplied by a legitimate, trusted entity. The reason for this extra measure is that, in its absence, an attacker could modify the system being checked for integrity and also make a corresponding modification to the control hash value so that the subsequent integrity check still passes. This control aims to ensure that only legitimate entities can supply control hash values for software and update packages.

The mission should have accountability of software/system components includes the system name, software owners, software version numbers, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). The Program should maintain a Software Bill of Materials (SBOM) for all software code utilized and continuously update/revise it for each step in the software lifecycle (to include the deployment of that software). The SBOM, as described in Executive Order 14028, “Improving the Nation's Cybersecurity,” encompasses the elements defined in the U.S. Department of Commerce the minimum elements for an SBOM.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactics: TAC-02: Execution

- Addresses NIST 800-53, Revision 5, cybersecurity control(s) CM-4(1), CM-7(8), CM-8, CM-14, RA-5, SA-10(1), SA-10(3), SA-10(4), SA-10(5), SA-10(6), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9), SI-2, SI-3, SI-7
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.3.2.4 Malware Protection

3.3.2.4.1 GR-MALW-01 Malware Protection Function

Principle:

- *Mission operated systems should employ malicious code protection mechanisms:*
  - *at information system entry and exit points*
  - *on system components*
  - *capable of performing real-time scans of files from external sources on endpoints devices and at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy to detect and eradicate malicious code including those inserted through the exploitation of information system vulnerabilities.*

- *Missions should incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes*

Rationale: Cyber actors utilize the execution of malicious code on mission systems to gain a foothold in the environment from which to gain persistence and carry out additional tactics to meet their campaign goals.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactics: TAC-02: Execution
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-4(14), AC-4(15), CM-11, IR-4(12), RA-5, SC-8(4), SC-18(5), SC-35, SC-44, SI-3, SI-7
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.3.2.5 Multi-Factor Authentication

3.3.2.5.1 GR-MFA-01 Risk-informed Use of Multi-Factor Authentication Function

Principle: *The mission should provide the capability for each system owner to implement Multi-Factor Authentication of a specific level of assurance.*

Rationale: Multi-Factor Authentication provides an additional level of assurance to interdict cyber actors who have already compromised a given user's password. In the case of strong, phishing resistant MFA certain cyber actor techniques such as man-in-the-middle can be effectively mitigated. In each of the following situations MFA should be employed:

- network access to privileged accounts
- network access to non-privileged accounts
- network access to applications and services
- local access to privileged accounts

- local access to non-privileged accounts

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities: CAP-01: Ability to Access Networks
- Interdicts Earliest Threat Actor Tactics: TAC-04: Privilege Escalation
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) IA-2(1), IA-2(2)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.3.2.6 Monitoring

3.3.2.6.1 GR-MON-01 Unique Identifiers for Authentication Function

Principle: *The mission should define the indicators of users (including those categorized as privileged users) posing a significant risk in a mission-specific context.*

Rationale: The mission should use these indicators on contextual information to monitor for user actions that collectively indicate a further investigation by security analysts is warranted and triggered. Credential compromise and insider threat can both result in actions that appear to meet basic access policy and pass standard technical controls. Monitoring for anomalies in user behavior allows for earlier detection of these cyber actor tactics. This control focuses on the Zero Trust eXtended Ecosystem element of PEOPLE.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities: CAP-01: Ability to Access Networks
- Interdicts Earliest Threat Actor Tactics: TAC-05: Evasion
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-2(12), AC-2(13), AT-2(2), AT-2(4), CA-2(2), IR-4(6), IR-4(7), IR-4(13), PM-12, SI-4(19), SI-4(20)
- Addresses PREVENT Space Mission Security and Protection Pillar

3.3.2.6.2 GR-MON-02 Risk-informed Authorization for Non-Mission Users Function

Principle: *The mission should design for capabilities to detect inappropriate or malicious activity within the mission's systems as soon as possible and provide alerts upon detection.*

Rationale:

- Early detection of cyber actor activity on end user devices and hosts running workloads is critical to limiting the impact of those activities as closely to their initial point of entry. Therefore, the mission should provide the capability for each system owner to provide mission-defined host-based monitoring mechanisms on mission-defined information system components.
- Monitoring information systems at the operating system and workload/application level is often the last line of defense against cyber actor activities design to impact mission capabilities in the form of exfiltration of, denial of access to, or modification of mission critical data and its support for business/production processes. Therefore, the mission should: monitor the use of information system accounts; provide the capability for each system owner to identify unauthorized use of the information system through mission-defined techniques and methods; and provide the capability for each system owner to detect network services that have not been authorized or approved by mission-defined authorization or approval processes.

This control focuses on the Zero Trust eXtended Ecosystem element of DEVICES and WORKLOADS.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability:
  - CAP-02: Ability to Discover and Exploit Vulnerabilities
  - CAP-03: Ability to Defeat Cryptography and Authentication
- Interdicts Earliest Threat Actor Tactic:
  - TAC-02: Execution
  - TAC-05: Evasion
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-2(3), AC-2(4), AC-2(6), AC-2(11), AC-2(12), AC-2(13), SA-4(9), SA-9(2), SI-4, SI-4(22), SI-4(23)
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.3.2.6.3 GR-MON-03 Network and Communications Monitoring Function

Principle: *The mission should provide the capability for each system owner to monitor communications at the external boundary of the system and at mission critical internal boundaries within the system.*

Rationale: The mission should provide the capability for each system owner to allow for enterprise level monitoring for unauthorized local network connections. The mission should make provisions so that program-defined encrypted communications traffic is visible to mission-defined information system monitoring tools. The mission should provide the capability for each system owner to analyze collected outbound communications traffic to identify anomalies. The mission should provide the capability for each system owner to monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. Early detection of cyber actor command and control communications, attempts to explore or move laterally within the environment, or to exfiltrate data require comprehensive network and communications monitoring and analysis. This control focuses on the Zero Trust eXtended Ecosystem element of NETWORKS.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-04: Command and Control Sophistication
- Interdicts Earliest Threat Actor Tactic: TAC-09: Command and Control
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) SC-7, SC-31, SI-4, SI-4(4), SI-4(10), SI-4(11), SI-4(15), SI-4(18)
- Addresses MITIGATE Space Mission Security and Protection Pillar

3.3.2.6.4 GR-MON-04 Cyber Activity Response and Reporting Function

Principle: *The mission should develop parameters to describe normal activities on the network for accessing and controlling mission applications and capabilities in a manner that allows security operations incident response and leadership to make effective decisions about resource allocation and risk management.*

Rationale:
These parameters should guide decisions about where and when to employ automated response and reporting mechanisms

- Normal network activity parameters should be developed by security analysts and mission experts working together to describe quantitatively what currently known patterns of network traffic look like. These parameters can be used to craft automated rules to trigger alerts and changes to network security controls.
- Automated alerting that brings high-quality information of possible cyber actor activities directly to the attention of security analysts is a critical capability required to tighten the loop between initial access by cyber actors and the containment, eradication, and recovery response activities. Therefore, the mission should employ automated mechanisms to alert security personnel of anomalous, inappropriate, or unusual activities with security implications that meet a certain threshold of confidence and potential impact based on analysis.
- Regular and systematic reporting of internally developed threat intelligence allows for the appropriate adjustments to mission-wide risk thresholds and risk response decisions. Therefore, the mission should report identified indications of mission-defined inappropriate or unusual activity to mission-defined personnel or role.

This control focuses on the Zero Trust eXtended Ecosystem element of AUTOMATION and REPORTING.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capability: CAP-01: Ability to Access Networks
- Interdicts Earliest Threat Actor Tactic: TAC-01: Initial Access
- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AU-6, SI-4(12), SI-4(14)
- Addresses MITIGATE and RECOVER Space Mission Security and Protection Pillar

3.3.2.7 Software Restriction

3.3.2.7.1 GR-SOFT-01 Software Installation Function

Principle: *The mission should provide the capability for each system owner to configure the flight and ground system to require a user to possess an explicit identified privilege to install software.*

Rationale: The mission should provide the capability for each system owner to configure the flight and ground system to prevent the installation or upgrades to software and firmware without verification that the component has been digitally signed using a certificate that is recognized, has not been revoked, and is approved by the organization. The mission should provide the capability for each system owner to configure the flight and ground system to prevent mission execution in accordance with mission-defined policies regarding software mission usage and restrictions. The mission should enforce software installation policies through mission-defined methods (such as a centrally managed application whitelisting capability) managed by software development, procurement, deployment, configuration, patching, and retirement processes].

Cyber actor attack sequences which rely on end users to trigger installation of malicious software can be interdicted by controls which validate and restrict operating system, browser, application, and other software installation.

This Principle Addresses These Controls:

- Addresses Primary Threat Actor Capabilities: CAP-02: Ability to Discover and Exploit Vulnerabilities
- Interdicts Earliest Threat Actor Tactics: TAC-02: Execution

- Addresses NIST 800-53, Revision 5, cybersecurity control(s) AC-3(12), CM-2, CM-3(3), CM-7(6), CM-7(2), CM-11, CM-11(2), CM-11(3), CM-14, SI-7(12), SI-7(15)
- Addresses PREVENT Space Mission Security and Protection Pillar

A. APPENDIX A – ACRONYMS AND ABBREVIATIONS

Acronym	Term
AC	Access Control
AO	Authorizing Official
API	Application Programming Interface
ATO	Authorization to Operate
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BPG	Best Practices Guide
CA	Assessment, Authorization, and Monitoring (NIST 800.53)
CAP	Capability
CJCSI	Chairman of the Joint Chiefs of Staff
CND	Computer Network
COMSEC	COMmunications SECurity
COOP	COntinuity of OPerations
DOD	Department of Defense
DODI	Department of Defense Instruction
EPB	Enterprise Protection Board
EPP	Enterprise Protection Program
ESDMD	Exploration Systems Development Mission Directorate
FIPS	Federal Information Processing Standard
FOD	Flight Operations Directorate
GB	Guide Book
GSFC	Goddard Space Flight Center
GNSS	Global Navigation Satellite System
GP	Gateway Payload
IA	Information Assurance
IA	Identification and Authentication (NIST 800.53)
ICS	Industrial Control Systems
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Incident Response
ITAR	International Traffic in Arms Regulations
JPL	Jet Propulsion Laboratory
KPP	Key Performance Parameter
MA	Maintenance
MCC	Mission Control Center
MFA	Multi-Factor Authentication
MITRE	Massachusetts Institute of Technology Research and Engineering
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCE	Office of the Chief Engineer

Acronym	Term
OCIO	Office of the Chief Information Officer
OPSEC	OPerational SECurity
OSMA	Office of Safety and Mission Assurance
OT	Operational Technologies
PE	Physical and Environment Protection
PM	Program Management
PNT	Positioning, Navigation, and Timing
RA	Risk Assessment
RFI	Radio Frequency Interference
SBOM	Software Bill of Materials
SC	System and Communications Protection
SI	System and Information Integrity
SMD	Science Mission Directorate
SOMD	Space Operations Mission Directorate
SR	Supply Chain Risk Management (NIST 800.53)
SSP	System Security Plan
STD	Standard
STMD	Space Technology Mission Directorate
TAC	Tactic
TOR	Terms of Reference
VoIP	Voice over Internet Protocol
VTC CODEC	Video TeleConferencing COmpression-Decompression

B. APPENDIX B – PRINCIPLES IMPLEMENTATION MATRIX

Principle Number	Principle Title	Principle Statement	Implementable Yes/No	Verification/Validation of Implementation	If Not Able to Implement What Would It Take	Comments
GV-RSK-01	Adaptive Risk Response & Resource Allocation Function	As a best practice the mission should establish a continuous process of qualitative and quantitative mission security risk analysis and risk response for the duration of the mission.				
MI-ARCH-01	Mission Least Privilege Function	The mission should establish and maintain a current and accurate data flow diagram covering mission essential data flows, including those that pass-through mission-external service providers.				
MI-ARCH-02	Mission Essential Data Flow Function	The mission should employ the principles of domain separation and least privilege for the on-board architecture, communications, and control.				
MI-AUTH-01	Boundary Protection Function	The mission should establish a mediated access mechanism that prevents unauthorized access to critical subsystems in the space segment.				
MI-AUTH-02	Comprehensive Authentication and Authorization Function	The mission should ensure only authenticated and authorized personnel, devices, and software are allowed to access the space mission system.				
MI-INTG-01	Communications Survivability Function	The mission should be able to recover from communications jamming and spoofing attempts.				
MI-INTG-02	PNT Survivability Function	The mission should be able to recover from positioning, navigation, and timing jamming and spoofing attempts.				
MI-SOFT-01	Software Mission Assurance Function	The mission should perform software assurance via established procedures and technical methods.				
MI-SOFT-02	Software and Hardware Testing Function	The mission should establish procedures and technical methods to perform end to end testing to include negative testing (i.e., abuse cases) of the mission hardware and software as it would be in an operating state (test as you fly).				
MI-MALW-01	Mission Malware Protection Function	The mission system software updates should be validated as free from malware prior to deployment, launch, and at defined regular intervals while the mission is in operations.				
MI-MALW-02	Mission Software, Programmable Logic Devices, and Firmware Integrity Function	The mission should establish and verify the integrity of its software images.				
MI-DCO-01	Mission Adversarial Actions Detection Function	The mission should incorporate an on-board adversarial actions detection function in its requirements and resulting system.				
MI-DCO-02	Mission Fault Management	The mission should incorporate fault management bypass protection in its requirements and resulting system.				
MI-MA-01	Mission Recovery Function	The mission should include intentional disruptions consistent with the mission threat analysis in anomaly detection, response, and recovery plans and designs in the flight segment and ground segment.				
MI-MA-02	Cyber-Safe State Function	The mission should design secure vehicle fault management functions and safe mode operations.				
GR-AUTH-01	Unique Identifiers for Authentication Function	The mission should provide the capability for each system to uniquely identify and authenticate organizational users and computing processes acting on behalf of organizational users.				
GR-AUTH-02	Risk-informed Authorization for Non-Program Users Function	The mission should use only verified identities when provisioning authenticators to organizational users and processes acting on behalf of users.				
GR-AUTH-03	Secure Workload-to-Workload Authenticator Function	The mission should define policy and procedures to ensure that the developed or delivered systems do not embed unencrypted static authenticators in applications, access scripts, configuration files, nor store unencrypted static authenticators on function keys.				
GR-DEVA-01	Computing Device Authentication Function	The mission should provide the capability to uniquely identify and authenticate all types of computing devices, including mobile devices and network connected endpoint devices (including workstations, printers, servers, VoIP Phones, VTC CODECs) before establishing a network connection. The mission should require developers of information systems, system components, or information system services to enable integrity verification of software and firmware components prior to delivery and during mission operations.				
GR-INTG-01	Software and Firmware Integrity Verification Function	Each system operated by the mission should provide the capability to verify the integrity of mission-defined software, firmware, and information. The mission should provide and employ integrity verification tools to detect unauthorized changes to mission-defined software, firmware, and information. The mission should define processes and procedures to be followed when integrity verification tools detect unauthorized changes to mission-defined software, firmware, and information.				
GR-MALW-01	Malware Protection Function	Mission operated systems should employ malicious code protection mechanisms: • at information system entry and exit points • on system components • capable of performing real-time scans of files from external sources on endpoints devices and at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy to detect and eradicate malicious code including those inserted through the exploitation of information system vulnerabilities The mission should incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.				
GR-MFA-01	Risk-informed Use of Multi-Factor Authentication Function	The mission should provide the capability for each system owner to implement Multi-Factor Authentication of a specific level of assurance.				
GR-MON-01	Unique Identifiers for Authentication Function	The mission should define the indicators of users (including those categorized as privileged users) posing a significant risk in a mission-specific context.				
GR-MON-02	System-based Monitoring & Alerting Function	The mission should design for capabilities to detect inappropriate or malicious activity within the mission's systems as soon as possible and provide alerts upon detection.				
GR-MON-03	Network and Communications Monitoring Function	The mission should provide the capability for each system owner to monitor communications at the external boundary of the system and at mission critical internal boundaries within the system.				
GR-MON-04	Threat Activity Response & Reporting Function	The mission should develop parameters to describe normal activities on the network for accessing and controlling mission applications and capabilities in a manner that allows security operations incident response and leadership to make effective decisions about resource allocation and risk management.				
GR-SOFT-01	Software Installation Function	The mission should provide the capability for each system owner to configure the system to require a user to possess an explicit identified privilege to install software.				

C. APPENDIX C – NASA STANDARD 1006 W/ CHANGE 1

Latest version can be found at: https://standards.nasa.gov/standard/NASA/NASA-STD-1006

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

NASA-STD-1006 W/CHANGE 1

DOCUMENT HISTORY LOG

Status	Document Revision	Change Number	Approval Date	Description
Baseline			2019-10-29	Initial Release
	Change	1	2020-11-05	Administrative/Editorial Change: Clarified SSPR 1 requirement, tailoring, and guidance; updated SSPR 4 guidance; added administrative updates for policy and organizational references; changed Space Asset Protection Program (SAPP) to Mission Resilience and Protection Program (MRPP).

NASA-STD-1006 W/CHANGE 1

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 will 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 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 — November 5, 2020

Ralph R. Roe, Jr.
NASA Chief Engineer

Approval Date

APPROVED FOR PUBLIC RELEASE—DISTRIBUTION IS UNLIMITED

NASA-STD-1006 W/CHANGE 1

TABLE OF CONTENTS

NASA-STD-1006 W/CHANGE 1

LIST OF APPENDICES

NASA-STD-1006 W/CHANGE 1

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. This NASA Technical Standard implements the requirements for protecting space systems in NASA Interim Directive (NID) 1058.127, NASA Enterprise Protection Program, NID 7120.130, NASA Space Flight Program and Project Management Requirements - Space Systems Protection Standard Update, and NPR 7120.8, NASA Research and Technology Program and Project Management Requirements.

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 will 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 to the extent specified or referenced in applicable contracts, grants, or agreements.

Verifiable requirement statements are 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 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.

NASA-STD-1006 W/CHANGE 1

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 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)

NID 1058.127	NASA Enterprise Protection Program
NID 1600.55	Sensitive But Unclassified (SBU) Controlled Information
NID 7120.130	NASA Space Flight Program and Project Management Requirements – Space Systems Protection Standard
NPR 2810.1	Security of Information Technology
NPR 7120.5	NASA Space Flight Program and Project Management Requirements
NPR 7120.8	NASA Research and Technology Program and Project Management Requirements
FIPS 140	Security Requirements for Cryptographic Modules, Level 1 (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
MRPP	Mission Resilience and Protection Program
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NESC	NASA Engineering and Safety Center
NID	NASA Interim Directive
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
PNT	Positioning, Navigation, and Timing
RF	Radio Frequency
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, Level 1.

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. This protection may be provided either via encryption (preferred) or authentication.*

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.*

v. *This requirement does not apply to balloon or sounding rocket projects.*

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; therefore, missions should implement both encryption and authentication to the extent possible.*
ii. *Missions can select an appropriate encryption scheme for each leg of the command path, e.g., SOC->MOC->Tracking 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. All missions should implement CCSDS 232.1-B-2, Communications Operations Procedure-1; but by itself, CCSDS 232.1-B-2 is insufficient to meet this requirement.*

4.1.2 Backup Command Link Protection

[SSPR 2] If a project uses an encrypted primary command link, any backup command link shall at 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 Mission Resilience and Protection Program (MRPP) 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 Ensure 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:

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 NASA Engineering and Safety Center (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 Interfaces.*

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. 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.

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 considerations 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 MRPP 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 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.

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 MRPP via NASA-DL-EMI-REPORT@mail.nasa.gov.*

vi. *MRPP, in coordination with the Enterprise Protection Program (EPP), will maintain a registry 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.

NASA-STD-1006 W/CHANGE 1

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 W/CHANGE 1				
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, Level 1.		
4.1.2	Backup Command Link Protection	[SSPR 2] If a project uses an encrypted primary command link, any backup command link shall at 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	Ensure 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 MRPP or to other designated notifying organizations.		

NASA-STD-1006 W/CHANGE 1

NASA-STD-1006 W/CHANGE 1				
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.		

NASA-STD-1006 W/CHANGE 1

APPENDIX B

REFERENCES

B.1 Purpose/Scope

This Appendix provides reference information to the user.

B.2 Reference Document

	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 232.1-B-2	Communications Operations Procedure-1
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 System Directorate, Systems Engineering and Integation, Interface Specification, Navstar GPS Space Segment/Navigation User Interfaces (https://www.gps.gov)
MSFC Form 4657	Change Request for a NASA Engineering Standard

D. APPENDIX D – NIST 800-53 REV 5 APPLICABLE CONTROLS

NIST 800-53 Rev 5 Control	Control Title	Control	Related Controls	Control Enhancements
ACCESS CONTROL				
AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes	AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37	• AC-2(3): DISABLE ACCOUNTS - Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period]. • AC-2(4): AUTOMATED AUDIT ACTIONS - Automatically audit account creation, modification, enabling, disabling, and removal actions. • AC-2(6): DYNAMIC PRIVILEGE MANAGEMENT - Implement [Assignment: organization-defined dynamic privilege management capabilities]. • AC-2(11): USAGE CONDITIONS - Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts]. • AC-2(12): ACCOUNT MONITORING FOR ATYPICAL USAGE - (a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and (b) Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles]. • AC-2(13):DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS - Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].
AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8	• AC-3(12): ASSERT AND ENFORCE APPLICATION ACCESS (a) Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions]; (b) Provide an enforcement mechanism to prevent unauthorized access; and (c) Approve access changes after initial installation of the application.
AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].	AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31	• AC-4(2): PROCESSING DOMAINS - Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions. • AC-4(3): DYNAMIC INFORMATION FLOW CONTROL - Enforce [Assignment: organization-defined information flow control policies]. • AC-4(6): METADATA - Enforce information flow control based on [Assignment: organization-defined metadata]. • AC-4(13): DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS - When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms • AC-4(14): SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS - When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content. • AC-4(15): DETECTION OF UNSANCTIONED INFORMATION - When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy]. • AC-4(21): PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS - Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].
AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38	None
AWARENESS AND TRAINING				
AT-2	Literacy Training And Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined events]; b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]; c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16	• AT-2(2): INSIDER THREAT - Provide literacy training on recognizing and reporting potential indicators of insider threat. • AT-2(4): SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR - Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].
AUDIT AND ACCOUNTABILITY				
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring auditrelated information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organizationdefined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11	None
AU-3	Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.	AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11	None
AU-4	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].	AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4	None
AU-5	Response to Audit Logging Process Failures	a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and b. Take the following additional actions: [Assignment: organization-defined additional actions].	AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12	None
AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7	None
AU-8	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	AU-3, AU-12, AU-14, SC-45	None
AU-9	Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.	AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4	None
AU-14	Session Audit	a. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; and b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable	AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12	None
ASSESSMENT, AUTHORIZATION, AND MONITORING				
CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3	• CA-2(2): SPECIALIZED ASSESSMENTS - Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].
CA-3	Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [Assignment: organization-defined frequency].	AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12	• CA-3(6): TRANSFER AUTHORIZATIONS - Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.
CA-8	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	RA-5, RA-10, SA-11, SR-5, SR-6	None
CONFIGURATION MANAGEMENT				
CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and 3. When system components are installed or upgraded.	AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18	None
CM-3	Configuration Change Control	a. Determine and document the types of changes to the system that are configurationcontrolled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].	CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11	• CM-3(2): TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES - Test, validate, and document changes to the system before finalizing the implementation of the changes. • CM-3(3): AUTOMATED CHANGE IMPLEMENTATION - Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms]. • CM-3(7): REVIEW SYSTEM CHANGES - Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred. • CM-3(8): PREVENT OR RESTRICT CONFIGURATION CHANGES - Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].

NIST 800-53 Rev 5 Control	Control Title	Control	Related Controls	Control Enhancements
CM-4	Impact Analysis	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2	• CM-4(1): SEPARATE TEST ENVIRONMENTS - Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-5	Access Restriction For Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10	None
CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].	AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4	• CM-7(4): UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION (a) Identify [Assignment: organization-defined software programs not authorized to execute on the system]; (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized software programs [Assignment: organization-defined frequency]. • CM-7(5): AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION (a) Identify [Assignment: organization-defined software programs authorized to execute on the system]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [Assignment: organization-defined frequency]. • CM-7(6): CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined userinstalled software]. • CM-7(8): BINARY OR MACHINE EXECUTABLE CODE (a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and (b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.
CM-8	System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and b. Review and update the system component inventory [Assignment: organization-defined frequency].	CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4	• CM-8(3): AUTOMATED UNAUTHORIZED COMPONENT DETECTION (a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].
CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	AC-17, AU-6, CM-7, CM-8, PM-30, SC-7	None
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].	AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7	• CM-11(2): SOFTWARE INSTALLATION WITH PRIVILEGED STATUS Allow user installation of software only with explicit privileged status. • CM-11(3): AUTOMATED ENFORCEMENT AND MONITORING Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].
CM-14	Signed Components	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	CM-7, SC-12, SC-13, SI-7	None
CONTINGENCY PLANNING				
CP-8	Telecommunication Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	CP-2, CP-6, CP-7, CP-11, SC-7	None
CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	CM-2, SA-8, SC-24, SI-13, SI-17	None
IDENTIFICATION AND AUTHENTICATION				
IA-2	Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8	• IA-2(1): MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS Implement multi-factor authentication for access to privileged accounts. • IA-2(2): MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS Implement multi-factor authentication for access to non-privileged accounts. • IA-2(5): INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources. • IA-2(8): ACCESS TO ACCOUNTS - REPLAY RESISTANT Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].
IA-3	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4	• IA-3(1): CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.
IA-4	Identifier Management	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for [Assignment: organization-defined time period].	AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37	• IA-4(4): IDENTIFY USER STATUS Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].
IA-5	Authenticator Management	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.	AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13	• IA-5(7): NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.
IA-8	Identification and Authentication (Non-Organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8	None
IA-9	Service Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	IA-3, IA-4, IA-5, SC-8	None
IA-10	Adaptive Authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	IA-2, IA-8	None
IA-11	Re-Authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	AC-3, AC-11, IA-2, IA-3, IA-4, IA-8	None
IA-12	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.	AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8	None
INCIDENT RESPONSE				
IR-4	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7	• IR-4(3): CONTINUITY OF OPERATIONS Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents]. • IR-4(5): AUTOMATIC DISABLING OF SYSTEM Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected. • IR-4(6): INSIDER THREATS Implement an incident handling capability for incidents involving insider threats. • IR-4(7): INSIDER THREATS — INTRA-ORGANIZATION COORDINATION Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities]. • IR-4(10): SUPPLY CHAIN COORDINATION Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain. • IR-4(12): MALICIOUS CODE AND FORENSIC ANALYSIS Analyze malicious code and/or other residual artifacts remaining in the system after the incident. • IR-4(13): BEHAVIOR ANALYSIS Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].
IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].	CM-6, CP-2, IR-4, IR-5, IR-8, IR-9	• IR-6(3): SUPPLY CHAIN COORDINATION Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
MAINTENANCE				
MA-3	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].	MA-2, PE-16	• MA-3(6): SOFTWARE UPDATES AND PATCHES Inspect maintenance tools to ensure the latest software updates and patches are installed.

NIST 800-53 Rev 5 Control	Control Title	Control	Related Controls	Control Enhancements
PHYSICAL AND ENVIRONMENTAL PROTECTION				
PE-2	Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Remove individuals from the facility access list when access is no longer required.	AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6	None
PE-3	Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards]; b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]; d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]; e. Secure keys, combinations, and other physical access devices; f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.	AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3	None
PROGRAM MANAGEMENT				
PM-9	Risk Management Strategy	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.	AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2	None
PM-10	Authorization Process	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Integrate the authorization processes into an organization-wide risk management program.	CA-6, CA-7, PL-2	None
PM-12	Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.	AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14	None
PM-28	Risk Framing	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]; and c. Review and update risk framing considerations [Assignment: organization-defined frequency].	CA-7, PM-9, RA-3, RA-7	None
PM-30	Supply Chain Risk Management Strategy	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; b. Implement the supply chain risk management strategy consistently across the organization; and c. Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.	CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11	• PM-30(1): SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.
PERSONNEL SECURITY				
PS-2	Position Risk Designation	a. Assign a risk designation to all organizational positions; b. Establish screening criteria for individuals filling those positions; and c. Review and update position risk designations [Assignment: organization-defined frequency].	AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12	None
RISK ASSESSMENT				
RA-3	Risk Assessment	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12	• RA-3(1): SUPPLY CHAIN RISK ASSESSMENT (a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and (b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.	CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11	• RA-5(2): UPDATE VULNERABILITIES TO BE SCANNED Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. • RA-5(3): BREADTH AND DEPTH OF COVERAGE Define the breadth and depth of vulnerability scanning coverage.
RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2	None
SYSTEM AND SERVICES ACQUISITION				
SA-3	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9	None
SA-4	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organizationdefined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria.	CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5	• SA-4(3): DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes: (a) [Assignment: organization-defined systems engineering methods]; (b) [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; and (c) [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes]. • SA-4(9): FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.
SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5	• SA-8(14): LEAST PRIVILEGE Implement the security design principle of least privilege in [Assignment: organizationdefined systems or system components].
SA-9	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5	• SA-9(2): IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].
SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organizationdefined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6	• SA-10(1): SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components. • SA-10(3): HARDWARE INTEGRITY VERIFICATION Require the developer of the system, system component, or system service to enable integrity verification of hardware components. • SA-10(4): TRUSTED GENERATION Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions. • SA-10(5): MAPPING INTEGRITY FOR VERSION CONTROL Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version. • SA-10(6): TRUSTED DISTRIBUTION Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

NIST 800-53 Rev 5 Control	Control Title	Control	Related Controls	Control Enhancements
SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all postdesign stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.	CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7	• SA-11(1): STATIC CODE ANALYSIS Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis. • SA-11(2): THREAT MODELING AND VULNERABILITY ANALYSES Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: (a) Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; (b) Employs the following tools and methods: [Assignment: organization-defined tools and methods]; (c) Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and (d) Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria]. • SA-11(4): MANUAL CODE REVIEWS Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques]. • SA-11(5): PENETRATION TESTING Require the developer of the system, system component, or system service to perform penetration testing: (a) At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; and (b) Under the following constraints: [Assignment: organization-defined constraints]. • SA-11(6): ATTACK SURFACE REVIEWS Require the developer of the system, system component, or system service to perform attack surface reviews. • SA-11(8): DYNAMIC CODE ANALYSIS Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. • SA-11(9): INTERACTIVE APPLICATION SECURITY TESTING Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.
SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].	MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9	• SA-15(5): ATTACK SURFACE REDUCTION Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds]. • SA-15(7): AUTOMATED VULNERABILITY ANALYSIS Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to: (a) Perform an automated vulnerability analysis using [Assignment: organization-defined tools]; (b) Determine the exploitation potential for discovered vulnerabilities; (c) Determine potential risk mitigations for delivered vulnerabilities; and (d) Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles]. • SA-15(8): REUSE OF THREAT AND VULNERABILITY INFORMATION Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process. • SA-15(11): ARCHIVE SYSTEM OR COMPONENT Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.
SA-17	Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture; b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.	PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7	• SA-17(7): STRUCTURE FOR LEAST PRIVILEGE Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.
SA-20	Customized Development of Critical Components	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].	CP-2, RA-9, SA-8	None
SA-21	Developer Screening	Require that the developer of [Assignment: organization-defined system, system component, or system service]: a. Has appropriate access authorizations as determined by assigned [Assignment: organizationdefined official government duties]; and b. Satisfies the following additional personnel screening criteria: [Assignment: organizationdefined additional personnel screening criteria].	PS-2, PS-3, PS-6, PS-7, SA-4, SR-6	None
SYSTEM AND COMMUNICATIONS PROTECTION				
SC-3	Security Function Isolation	Isolate security functions from nonsecurity functions.	AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16	None
SC-4	Information in Shared System	Prevent unauthorized and unintended information transfer via shared system resources.	AC-3, AC-4, SA-8	None
SC-5	Denial-of-Service Protection	a. [Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	CP-2, IR-4, SC-6, SC-7, SC-40	• SC-5(3): DETECTION AND MONITORING (a) Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; and (b) Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources].
SC-6	Resource Availability	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].	SC-5	None
SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43	• SC-7(3): ACCESS POINTS Limit the number of external network connections to the system. • SC-7(4): EXTERNAL TELECOMMUNICATIONS SERVICES (a) Implement a managed interface for each external telecommunication service; (b) Establish a traffic flow policy for each managed interface; (c) Protect the confidentiality and integrity of the information being transmitted across each interface; (d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need; (e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need; (f) Prevent unauthorized exchange of control plane traffic with external networks; (g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and (h) Filter unauthorized control plane traffic from external networks. • SC-7(5): DENY BY DEFAULT — ALLOW BY EXCEPTION Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]]. • SC-7(9): RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC (a) Detect and deny outgoing communications traffic posing a threat to external systems; and (b) Audit the identity of internal users associated with denied communications. • SC-7(10): PREVENT EXFILTRATION (a) Prevent the exfiltration of information; and (b) Conduct exfiltration tests [Assignment: organization-defined frequency]. • SC-7(11): RESTRICT INCOMING COMMUNICATIONS TRAFFIC Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations]. • SC-7(12): HOST-BASED PROTECTION Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components]. • SC-7(13): ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system. • SC-7(14): PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces]. • SC-7(15): NETWORKED PRIVILEGED ACCESSES Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing. • SC-7(16): PREVENT DISCOVERY OF SYSTEM COMPONENTS Prevent the discovery of specific system components that represent a managed interface. • SC-7(17): AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS Enforce adherence to protocol formats. • SC-7(18): FAIL SECURE Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device. • SC-7(19): BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS Block inbound and outbound communications traffic between [Assignment: organizationdefined communication clients] that are independently configured by end users and external service providers. • SC-7(20): DYNAMIC ISOLATION AND SEGREGATION Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components. • SC-7(21): ISOLATION OF SYSTEM COMPONENTS Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions]. • SC-7(22): SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS Implement separate network addresses to connect to systems in different security domains. • SC-7(28): CONNECTIONS TO PUBLIC NETWORKS Prohibit the direct connection of [Assignment: organization-defined system] to a public network. • SC-7(29): SEPARATE SUBNETS TO ISOLATE FUNCTIONS Implement [Selection: physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].
SC-8	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28	• SC-8(4): CONCEAL OR RANDOMIZE COMMUNICATIONS Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].
SC-18	Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.	AU-2, AU-12, CM-2, CM-6, SI-3	• SC-18(5): ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS Allow execution of permitted mobile code only in confined virtual machine environments.
SC-31	Covert Channel Analysis	a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b. Estimate the maximum bandwidth of those channels.	AC-3, AC-4, SA-8, SI-11	None

NIST 800-53 Rev 5 Control	Control Title	Control	Related Controls	Control Enhancements
SC-32	System Partitioning	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection: physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].	AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36	None
SC-35	External Malicious Code	Include system components that proactively seek to identify network-based malicious code or malicious websites.	SC-7, SC-26, SC-44, SI-3, SI-4	None
SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.	AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16	None
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	AC-18, SC-5	• SC-40(1): ELECTROMAGNETIC INTERFERENCE Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference. • SC-40(3): IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.
SC-44	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7	None
		SYSTEM AND INFORMATION INTEGRITY		
SI-2	Flaw Remediation	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organizationdefined time period] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.	CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11	None
SI-3	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organizationdefined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15	• SI-3(8): DETECT UNAUTHORIZED COMMANDS (a) Detect the following unauthorized operating system commands through the kernel application programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]; and (b) [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command].
SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10	• SI-4(1): SYSTEM-WIDE INTRUSION DETECTION SYSTEM Connect and configure individual intrusion detection tools into a system-wide intrusion detection system. • SI-4(2): AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS Employ automated tools and mechanisms to support near real-time analysis of events. • SI-4(4): INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC (a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organizationdefined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions]. • SI-4(10): VISIBILITY OF ENCRYPTED COMMUNICATIONS Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms]. • SI-4(11): ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies. • SI-4(12): AUTOMATED ORGANIZATION-GENERATED ALERTS Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts]. • SI-4(13): ANALYZE TRAFFIC AND EVENT PATTERNS (a) Analyze communications traffic and event patterns for the system; (b) Develop profiles representing common traffic and event patterns; and (c) Use the traffic and event profiles in tuning system-monitoring devices. • SI-4(14): WIRELESS INTRUSION DETECTION Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system. • SI-4(15): WIRELESS TO WIRELINE COMMUNICATIONS Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks. • SI-4(16): CORRELATE MONITORING INFORMATION Correlate information from monitoring tools and mechanisms employed throughout the system. • SI-4(17): INTEGRATED SITUATIONAL AWARENESS Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness. • SI-4(18): ANALYZE TRAFFIC AND COVERT EXFILTRATION Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system]. • SI-4(19): RISK FOR INDIVIDUALS Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk. • SI-4(20): PRIVILEGED USERS Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. • SI-4(22): UNAUTHORIZED NETWORK SERVICES (a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and (b) [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected. • SI-4(23): HOST-BASED DEVICES Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms]. • SI-4(24): INDICATORS OF COMPROMISE Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].
SI-7	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11	• SI-7(12): INTEGRITY VERIFICATION Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software]. • SI-7(15): CODE AUTHENTICATION Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organizationdefined information inputs to the system].	None	• SI-10(3): PREDICTABLE BEHAVIOR Verify that the system behaves in a predictable and documented manner when invalid inputs are received. • SI-10(4): TIMING INTERACTIONS Account for timing interactions among system components in determining appropriate responses for invalid inputs. • SI-10(5): RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats]. • SI-10(6): INJECTION PREVENTION Prevent untrusted data injections.
SI-17	Fail-Safe Procedures	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].	CP-12, CP-13, SC-24, SI-13	None
SI-21	Information Refresh	Refresh [Assignment: organization-defined information] at [Assignment: organizationdefined frequencies] or generate the information on demand and delete the information when no longer needed.	SI-14	None
		SUPPLY CHAIN RISK MANAGEMENT		
SR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; Systemlevel] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	PM-9, PM-30, PS-8, SI-12	None
SR-2	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]; b. Review and update the supply chain risk management plan [Assignment: organizationdefined frequency] or as required, to address threat, organizational or environmental changes; and c. Protect the supply chain risk management plan from unauthorized disclosure and modification.	CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4	None
SR-3	Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chainrelated events: [Assignment: organization-defined supply chain controls]; and c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organizationdefined document]].	CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11	• SR-3(2): LIMITATION OF HARM Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls]. • SR-3(3): SUB-TIER FLOW DOWN Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
SR-4	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4	• SR-4(4): SUPPLY CHAIN INTEGRITY — PEDIGREE Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or missionessential technologies, products, and services.
SR-7	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chainrelated information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].	SC-38	None
SR-9	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11	None

E. APPENDIX E – LIST OF PRINCIPLES

Principle	Principle Title	Principle Statement	Threat Actor Capability/Capabilities Addressed	Threat Actor Tactics Interdicted	NIST 800-53 Rev 5 Controls	Space Protection Pillar(s) Addressed
GV-RSK-01	Adaptive Risk Response & Resource Allocation Function	As a best practice the mission should establish a continuous process of qualitative and quantitative mission security risk analysis and risk response for the duration of the mission.	All Capabilities	All Tactics	PM-9, PM-28, RA-7	All Pillars
MI-ARCH-01	Mission Least Privilege Function	The mission should establish and maintain a current and accurate data flow diagram covering mission essential data flows, including those that pass-through mission-external service providers.	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-02: Execution	AC-4, AC-4(2), AC-4(3), AC-4(6), AC-4(21), CA-3, CA-3(6), SC-32	MITIGATE
MI-ARCH-02	Mission Essential Data Flow Function	The mission should employ the principles of domain separation and least privilege for the on-board architecture, communications, and control.	CAP-01: Ability to Access Networks	TAC-07: Lateral Movement	AC-3, AC-4, AC-6, SA-8(14), SA-17(7), SC-3, SC-4, SC-6, SC-7(20), SC-7(21), SC-39, SI-17	PREVENT
MI-AUTH-01	Boundary Protection Function	The mission should establish a mediated access mechanism that prevents unauthorized access to critical subsystems in the space segment.	CAP-01: Ability to Access Networks	TAC-12: Impact	SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(9), SC-7(10), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(15), SC-7(16), SC-7(17), SC-7(18), SC-7(19), SC-7(20), SC-7(21), SC-7(22), SC-7(28), SC-7(29)	PREVENT
MI-AUTH-02	Comprehensive Authentication and Authorization Function	The mission should ensure only authenticated and authorized personnel, devices, and software are allowed to access the space mission system.	• CAP-01: Ability to Access Networks • CAP-02: Ability to Discover and Exploit Vulnerabilities • CAP-05: Ability to Affect Cyber/Physical Systems • CAP-07: Sophistication of Human Influence	• TAC-01: Initial Access • TAC-02: Execution • TAC-04: Privilege Escalation	IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PE-3, PM-10, SI-7(15)	PREVENT
MI-DCO-01	Mission Adversarial Actions Detection Function	The mission should incorporate an on-board adversarial actions detection function in its requirements and resulting system.	CAP-04: Command and Control Sophistication	TAC-01: Initial Access	AC-4(15), AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-14, CM-8(3), RA-5(7), SC-5(3), SC-7(9), SI-3(8), SI-4(1), SI-4(2), SI-4(4), SI-4(10), SI-4(11), SI-4(12), SI-4(13), SI-4(14), SI-4(15), SI-4(16), SI-4(17), SI-4(18), SI-4(19), SI-4(20), SI-4(22), SI-4(23), SI-4(24)	MITIGATE
MI-DCO-02	Mission Fault Management	The mission should incorporate fault management bypass protection in its requirements and resulting system.	CAP-04: Command and Control Sophistication	TAC-01: Initial Access	AC-4(15), AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-14, CM-8(3), RA-5(7), SC-5(3), SC-7(9), SI-3(8), SI-4(1), SI-4(2), SI-4(4), SI-4(10), SI-4(11), SI-4(12), SI-4(13), SI-4(14), SI-4(15), SI-4(16), SI-4(17), SI-4(18), SI-4(19), SI-4(20), SI-4(22), SI-4(23), SI-4(24)	RECOVER
MI-INTG-01	Communications Survivability Function	The mission should be able to recover from communications jamming and spoofing attempts.	CAP-05: Ability to Affect Cyber/Physical Systems	TAC-10: Inhibit Response Function	CP-8, SC-5, SC-8, SC-40, SC-40(1), SC-40(3), SI-10(3), SI-10(5), SI-10(6)	RECOVER
MI-INTG-02	PNT Survivability Function	The mission should be able to recover from positioning, navigation, and timing jamming and spoofing attempts.	CAP-05: Ability to Affect Cyber/Physical Systems	TAC-10: Inhibit Response Function	AU-8, CP-8, SC-5, SC-40, SC-40(10), SC-40(3), SI-10(3), SI-10(4), SI-10(5), SI-10(6)	RECOVER
MI-MA-01	Mission Recovery Function	The mission should include intentional disruptions consistent with the mission threat analysis in anomaly detection, response, and recovery plans and designs in the flight segment and ground segment.	CAP-05: Ability to Affect Cyber/Physical Systems	TAC-10: Inhibit Response Function	CP-2(5), IR-4, SA-8(24)	RECOVER
MI-MA-02	Cyber-Safe State Function	The mission should design secure vehicle fault management functions and safe mode operations.	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-11: Impair Process Control	CP-12, SI-17, IR-4(3), IR-4(5)	RECOVER
MI-MALW-01	Mission Malware Protection Function	The mission system software updates should be validated as free from malware prior to deployment, launch, and at defined regular intervals while the mission is in operations.	CAP-05: Ability to Affect Cyber/Physical Systems	TAC-02: Execution	CM-4(1), CM-7(8), CM-14, RA-5, SA-10(1), SA-10(3), SA-10(4), SA-10(5), SA-10(6), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9), SI-2, SI-3, SI-71	MITIGATE
MI-MALW-02	Mission Software, Programmable Logic Devices, and Firmware Integrity Function	The mission should establish and verify the integrity of its software images.	CAP-05: Ability to Affect Cyber/Physical Systems	TAC-02: Execution	CM-4(1), CM-7(8), CM-14, RA-5, SA-10(1), SA-10(3), SA-10(4), SA-10(5), SA-10(6), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9), SI-2, SI-3, SI-7	MITIGATE
MI-SOFT-01	Software Mission Assurance Function	The mission should perform software assurance via established procedures and technical methods.	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-02: Execution	CA-8, CM-3(2), CM-3(7), CM-3(8), CM-4, CM-5, CM-7(4), CM-7(5), CM-10, IR-4(10), IR-6(3), MA-3(6), PM-30, PM-30(1), RA-3(1), SR-1, SA-4(3), SA-10(1), SA-15, SA-15(5), SA-15(7), SA-15(8), SA-15(11), SA(17), SA-20, SA-21, SI-2, SI-7, SR-9, SR-2, SR-3, SR-3(2)c, SR-3(3), SR-4(4), SR-7	PREVENT
MI-SOFT-02	Software and Hardware Testing Function	The mission should establish procedures and technical methods to perform end to end testing to include negative testing (i.e., abuse cases) of the mission hardware and software as it would be in an operating state (test as you fly).	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-02: Execution	CA-8, CM-3(2), RA-5, RA-5(2), RA-5(3), SA-3, SA-4(3), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9)	MITIGATE
GR-AUTH-01	Unique Identifiers for Authentication Function	The mission should provide the capability for each system to uniquely identify and authenticate organizational users and computing processes acting on behalf of organizational users.	• CAP-01: Ability to Access Networks • CAP-02: Ability to Discover and Exploit Vulnerabilities	• TAC-01: Initial Access • TAC-02: Execution	IA-2(5), IA-2(8), IA-5	PREVENT
GR-AUTH-02	Risk-informed Authorization for Non-Program Users Function	The mission should use only verified identities when provisioning authenticators to organizational users and processes acting on behalf of users.	CAP-05: Ability to Affect Cyber/Physical Systems	TAC-04: Privilege Escalation	IA-4(4), IA-8, IA-10, PM-10, PS-2, SI-4(19)	PREVENT
GR-AUTH-03	Secure Workload-to-Workload Authenticator Function	The mission should define policy and procedures to ensure that the developed or delivered systems do not embed unencrypted static authenticators in applications, access scripts, configuration files, nor store unencrypted static authenticators on function keys.	CAP-01: Ability to Access Networks	TAC-01: Initial Access	IA-5(7)	PREVENT
GR-DEVA-01	Computing Device Authentication Function	The mission should provide the capability to uniquely identify and authenticate all types of computing devices, including mobile devices and network connected endpoint devices (including workstations, printers, servers, VoIP Phones, VTC CODECs) before establishing a network connection.	CAP-01: Ability to Access Networks	TAC-01: Initial Access	IA-3, IA-3(1), CM-8	PREVENT
GR-INTG-01	Software and Firmware Integrity Verification Function	The mission should require developers of information systems, system components, or information system services to enable integrity verification of software and firmware components prior to delivery and during mission operations. Each system operated by the mission should provide the capability to verify the integrity of mission-defined software, firmware, and information. The mission should provide and employ integrity verification tools to detect unauthorized changes to mission-defined software, firmware, and information. The mission should define processes and procedures to be followed when integrity verification tools detect unauthorized changes to mission-defined software, firmware, and information.	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-02: Execution	CM-4(1), CM-7(8), CM-8, CM-14, RA-5, SA-10(1), SA-10(3), SA-10(4), SA-10(5), SA-10(6), SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(8), SA-11(9), SI-2, SI-3, SI-7	MITIGATE
GR-MALW-01	Malware Protection Function	Mission operated systems should employ malicious code protection mechanisms: • at information system entry and exit points • on system components • capable of performing real-time scans of files from external sources on endpoints devices and at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy to detect and eradicate malicious code including those inserted through the exploitation of information system vulnerabilities The mission should incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-02: Execution	AC-4(14), AC-4(15), CM-11, IR-4(12), RA-5, SC-8(4), SC-18(5), SC-35, SC-44, SI-3, SI-7	MITIGATE
GR-MFA-01	Risk-informed Use of Multi-Factor Authentication Function	The mission should provide the capability for each system owner to implement Multi-Factor Authentication of a specific level of assurance.	CAP-01: Ability to Access Networks	TAC-04: Privilege Escalation	IA-2(1), IA-2(2)	PREVENT
GR-MON-01	Unique Identifiers for Authentication Function	The mission should define the indicators of users (including those categorized as privileged users) posing a significant risk in a mission-specific context.	CAP-01: Ability to Access Networks	TAC-05: Evasion	AC-2(12), AC-2(13), AT-2(2), AT-2(4), CA-2(2), IR-4(6), IR-4(7), IR-4(13), PM-12, SI-4(19), SI-4(20)	PREVENT
GR-MON-02	System-based Monitoring and Alerting Function	The mission should design for capabilities to detect inappropriate or malicious activity within the mission's systems as soon as possible and provide alerts upon detection.	• CAP-02: Ability to Discover and Exploit Vulnerabilities • CAP-03: Ability to Defeat Cryptography and Authentication	• TAC-02: Execution • TAC-05: Evasion	AC-2(3), AC-2(4), AC-2(6), AC-2(11), AC-2(12), AC-2(13), SA-4(9), SA-9(2), SI-4, SI-4(22), SI-4(23)	MITIGATE
GR-MON-03	Network and Communications Monitoring Function	The mission should provide the capability for each system owner to monitor communications at the external boundary of the system and at mission critical internal boundaries within the system.	CAP-04: Command and Control Sophistication	TAC-09: Command and Control	SC-7, SC-31, SI-4, SI-4(4), SI-4(10), SI-4(11), SI-4(15), SI-4(18)	MITIGATE
GR-MON-04	Threat Activity Response and Reporting Function	The mission should develop parameters to describe normal activities on the network for accessing and controlling mission applications and capabilities in a manner that allows security operations incident response and leadership to make effective decisions about resource allocation and risk management.	CAP-01: Ability to Access Networks	TAC-01: Initial Access	AU-6, SI-4(12), SI-4(14)	MITIGATE AND RECOVER
GR-SOFT-01	Software Installation Function	The mission should provide the capability for each system owner to configure the system to require a user to possess an explicit identified privilege to install software.	CAP-02: Ability to Discover and Exploit Vulnerabilities	TAC-02: Execution	AC-3(12), CM-2, CM-3(3), CM-7(6), CM-7(2), CM-11, CM-11(2), CM-11(3), CM-14, SI-7(12), SI-7(15)	PREVENT

F. APPENDIX F – CHANGE REQUEST FORM

SPACE SECURITY: BEST PRACTICES GUIDE
CHANGE REQUEST

(EMAIL COMPLETED FORM TO HQ-DL-Mission-Security-BPG-Feedback@NASA.GOV)

REQUESTOR NAME

OFFICE

EMAIL

TYPE OF CHANGE BEING REQUESTED

ADDITION ☐ ***CHANGE*** ☐ ***IMPLEMENT*** ☐

PRINCIPLE NUMBER IF AVAILABLE

CHANGE BEING REQUESTED

If language changes to principle or rationale be explicit in the change being requested and the reasoning (i.e., change the sentence reading "the cow jumped over the moon" to "the cow while wearing a spacesuit on the lunar surface felt like it could jump over the moon, but bounced along the lunar surface due to low relative lunar gravity" due to cows not being able to breath in space and would require a spacesuit to do so, and lack a mechanism to effectively jump over the moon and would simply orbit, as this is not stated in the surrounding paragraph). If the suggestion is to implement, please provide justification and potential implementation guidance.