NIST IR
NIST IR 8401 ipd

Satellite Ground Segment:

Applying the Cybersecurity Framework to Assure Satellite Command and Control

Initial Public Draft

Suzanne Lightman
Theresa Suloway
Joseph Brule

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8401.ipd

National Institute of Standards and Technology
U.S. Department of Commerce

NIST IR
NIST IR 8401 ipd

Satellite Ground Segment:

Applying the Cybersecurity Framework to Assure Satellite Command and Control

Initial Public Draft

Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Theresa Suloway
Joseph Brule
The MITRE Corporation
McLean, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8401.ipd

April 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8401
Initial Public Draft
68 pages (April 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8401.ipd

Public comment period: April 18, 2022 – June 20, 2022

Submit comments on this publication to: pnt-eo@list.nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Space operations are increasingly important to the national and economic security of the United States. Commercial space's contribution to the critical infrastructure is growing in both volume and diversity of services, as illustrated by the increased use of commercial communications satellite (COMSAT) bandwidth, the purchase of commercial imagery, and the hosting of government payloads on commercial satellites. The U.S. Government recognizes and supports space resilience through numerous space policies, executive orders, and the National Cyber Strategy. The space cyber-ecosystem is an inherently risky, high-cost, and often inaccessible environment consisting of distinct yet interdependent segments. This report applies the NIST Cybersecurity Framework to the ground segment of space operations with an emphasis on the command and control of satellite buses and payloads.

Keywords

control; critical infrastructure; Cybersecurity Framework; ground segment; risk management; space operations; telemetry; tracking.

Acknowledgments

This publication is the result of a collaborative effort involving stakeholders throughout the world, including industry, academia, and government. NIST launched the project by hosting a series of biweekly workshops throughout the second half of 2021. The authors wish to thank all individuals and organizations that contributed to the creation of this document, including:

- Anne Aouizerate, Airbus
- Felipe Fernandez, Fortinet
- Jeff Finke, The MITRE Corporation
- Bertrand Leconte, Airbus
- Nicholas Martin, Lockheed Martin Space
- Stephen McCauley, Kratos Defense & Security Solutions
- Richard D. Newbold, EPRi
- Oliver Rossi, Airbus
- Chelsea J. Smethurst, Microsoft
- Nicholas Tsamis, The MITRE Corporation
- Shelly Waite-Bey
- Matt Young, Utah State University Space Dynamics Laboratory

Supplemental Content and Potential Updates

Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the NIST Interagency or Internal Report (NISTIR) 8401 publication details.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: pnt-eo@list.nist.gov.

Executive Summary

As stated in the September 2018 United States National Cyber Strategy, the U.S. Government (USG) considers unfettered access and freedom to operate in space vital to the advancement of the security, economic prosperity, and scientific knowledge of the Nation, and it is concerned with the growing cyber-related threats to space assets and their supporting infrastructure [NCS-2018]. The USG issued Space Policy Directive 5 (SPD-5) in 2020, which establishes key cybersecurity principles to guide and serve as the foundation for the Nation's approach to the cyber protection of space systems. SPD-5 also fosters practices within the USG and commercial space operations that protect space assets and their supporting infrastructure from cyber threats [SPD-5].

The intent of this document is to apply the Cybersecurity Framework to the creation of a Profile for the space sector's ground segment. The Profile provides a flexible framework for stakeholders to manage risks. Organizations are encouraged to make their risk management decisions in the context of their own cyber ecosystem, architecture, and risk tolerance. The goal of the profile is to supplement preexisting resilience measures and elevate the postures of less mature initiatives.

The Profile defined in this report helps address SPD-5's goals for securing space. It directly supports key principles, such as developing and implementing cybersecurity plans, to ensure space systems' ability to verify the integrity, confidentiality, and availability of critical functions, as well as retain or recover positive control of space vehicles.

The ground segment Profile is voluntary and does not issue regulations, define mandatory practices, provide a checklist for compliance, or carry statutory authority. It is intended to be a foundational set of guidelines.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

Space is an increasingly important element of the Nation's critical infrastructure. A loss or degradation of space services could significantly impact the security and economic well-being of the United States. The United States Government (USG) recognizes that government-owned space operations can be augmented through activities such as the leasing of commercial communications satellite (COMSAT) bandwidth, the use of commercial space-based telecommunication services, the purchase of commercial imagery, and the use of commercial satellite buses to host payloads and other capabilities.

To protect this sector, the National Institute of Standards and Technology (NIST) has developed this Profile under the Cybersecurity Framework to assist the operators of the commercial ground segment of the space sector in providing cybersecurity for their systems. The NIST Cybersecurity Framework [NIST-CSF] provides a means for stakeholders to assess their cybersecurity posture in terms of identification, protection, detection, response, and recovery operations and to derive a plan to elevate risk posture.

The scope of this document is the operational phase of the commercial space ground segment. Though the scope is defined as the ground segment, it is acknowledged that the cybersecurity requirements of the space segment may impact the ground segment. Space vehicles have severe size, weight, and power (SWaP) constraints, and it may be impractical to implement some cybersecurity controls on the satellite itself. The consideration of measures to enable the ground segment to improve its security posture on behalf of space vehicles is warranted. Stakeholders are referred to other documents for further guidance on securing the space vehicle [NIST-IR8270] and user [NIST-IR8323] segments.

1.1 Purpose and Objectives

The Satellite Ground Segment Cybersecurity Profile (herein referred to as the Profile) is designed to be used as part of a risk management program to help organizations manage cybersecurity risks to systems, networks, and assets that comprise the ground segment of satellite operations. The Profile provides guidance for:

- Classifying systems, processes, and components of satellite command, control, and payload systems in order to determine cybersecurity risk posture and address residual risk in the management and control of the space segment;
- Defining a desired cybersecurity state for the systems, processes, and components of satellite command, control, and payload systems; and
- Establishing defined and repeatable risk management approaches to elevate an actual cybersecurity state to a desired cybersecurity state.

The Profile does not serve as a compliance checklist that would guarantee some level of residual risk.

Use of the Profile will help organizations:

- Identify their systems and processes that enable command and control of space vehicle buses and payloads and determine performance requirements;

- Identify known and anticipated threats to the satellite ground segment and supporting infrastructure;
- Protect the systems that the ground segment relies on through policy, training, resilience, and access control;
- Detect a loss of ground segments' confidentiality, integrity, or availability;
- Respond to confidentiality breaches of Telemetry, Tracking, and Command (TT&C) and a manipulation or loss of satellite commands or telemetry in a timely, effective, and resilient manner; and
- Recover from anomalies in a timely, effective, and resilient manner.

1.2 Scope

The baseline profile focuses on two components of the satellite ground segment, as depicted on the left side of Figure 1:

1. The Mission Operations Center (MOC) that issues commands to a satellite control data handling platform and receives telemetry from a space vehicle's bus and
2. The Payload Control Center (PCC) that may issue commands to and receive responses from a payload that is hosted on a different organization's bus (i.e., the payload is residing on a space vehicle where the space vehicle bus operations are executed by an independent MOC).[1]

[1] A payload may have an independent PCC with the ability to issue commands and receive telemetry via a dedicated radio frequency (RF) link, or the payload may receive commands and send telemetry to the PCC by routing through the satellite bus and the MOC.

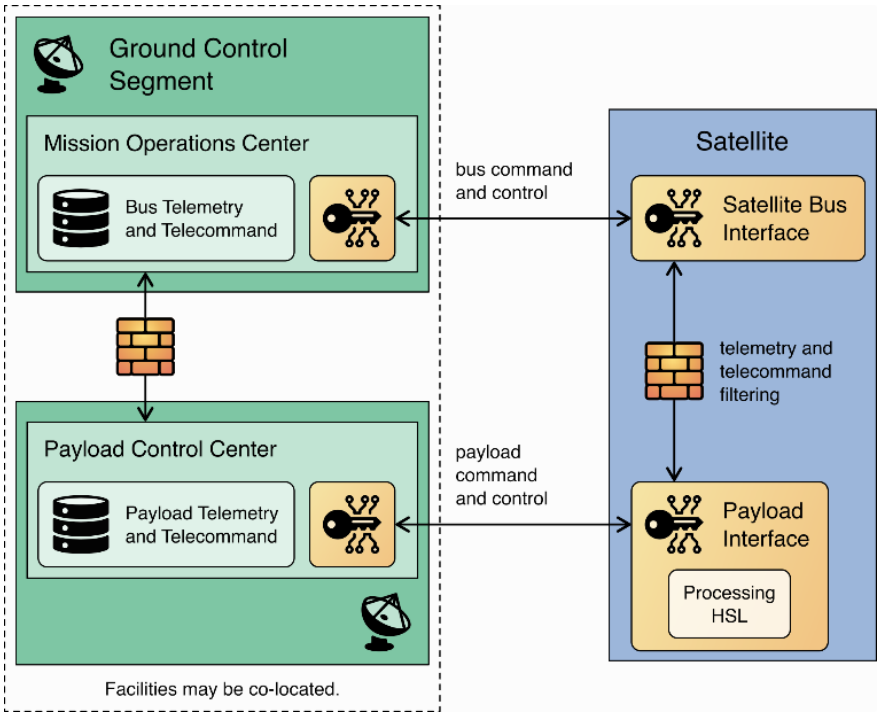

Figure 1 - Satellite Ground Segment Components of Commercial Space Operations

Figure 2 shows which components are in and out of scope for the Profile.

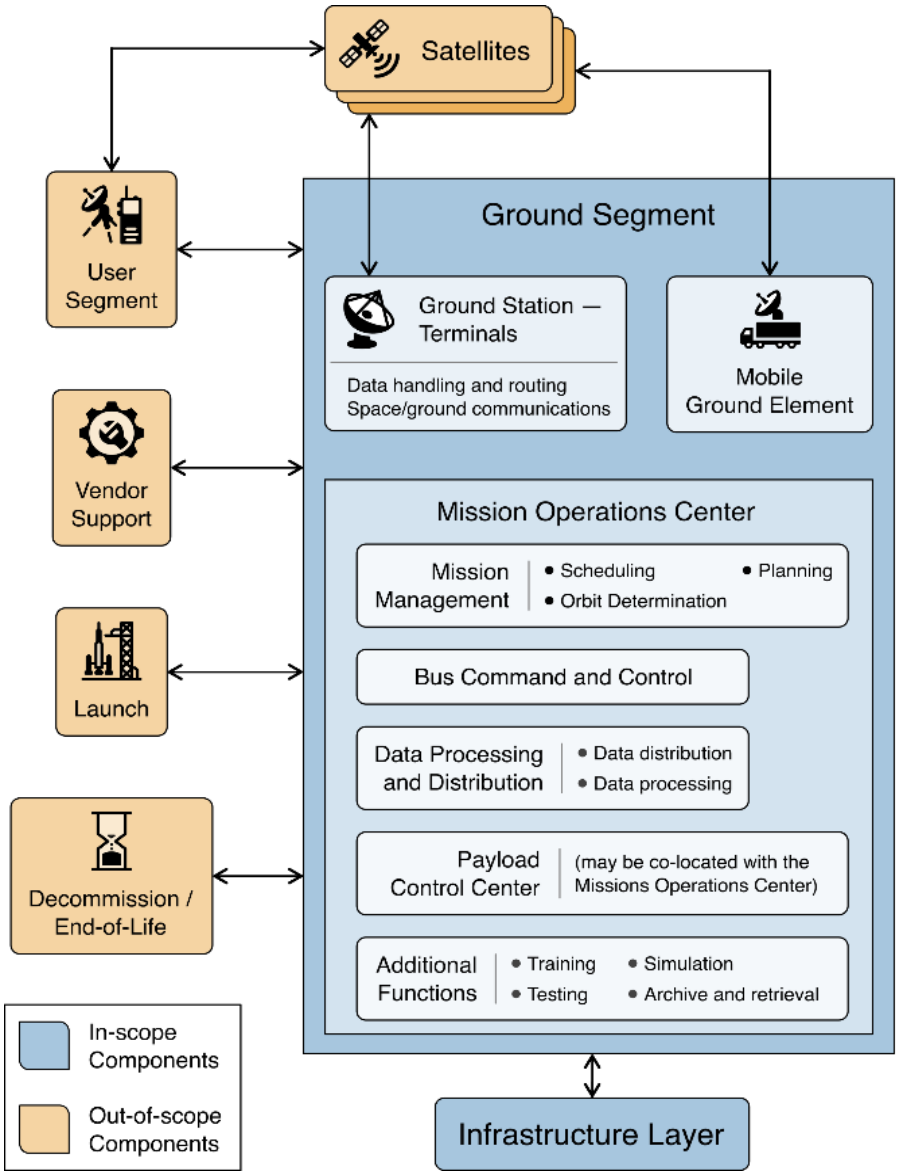

Figure 2 - Components In and Out of Scope for the Profile

The Profile will support the stakeholder's ability to:

- Make risk-informed decisions about the cybersecurity of the ground segment and its corresponding impact on the space segment's bus and payload,
- Select risk-based approaches that minimize the potential effects of the disruption or manipulation of satellite bus and payload commanding and telemetry, and
- Consider planning and action regarding the secure management and recovery of the space segment.

1.3 Audience

The intended audience includes public and private organizations that own, operate, or manage space systems and are seeking to assess or elevate their current security posture, such as:

- Risk managers, cybersecurity professionals, and others with a role in risk management for ground systems, and
- Researchers and analysts who study space systems and the unique cybersecurity needs of the space cyber-ecosystem.

The Profile is suitable for a range of stakeholders with varying degrees of risk management experience, including organizations with the following characteristics:

- Have already adopted the NIST Cybersecurity Framework to help identify, assess, and manage cybersecurity risks [NIST-CSF];
- Are familiar with the Cybersecurity Framework and want to improve their risk posture; or
- Are unfamiliar with the Cybersecurity Framework but need to implement or augment risk management efforts.

2 Intended Use

The Profile is a flexible tool that an organization can use as part of its risk management effort. This Profile is intended to augment rather than replace these efforts.

The Profile will aid in the prioritization of cybersecurity activities based on business objectives and identify areas where standards, practices, and other guidance could help manage risks. NIST also encourages the development of organization-specific profiles by applying this profile to a particular mission or cyber-ecosystem. Considerations for specific profiles include:

1. What ground segment processes and assets are dependent on other assets (i.e., what are the externalities and secondary effects)?
2. What is the level of interconnectivity (logical and physical) of the ground segment with other processes?
3. What processes and assets are vulnerable?
4. What are the integrity and availability thresholds to avoid mission impact?
5. What are the confidentiality requirements?
6. What safeguards are currently in place?
7. What is the impact to the organization should a process or asset be lost or degraded?
8. What techniques can be used to detect events of concern?
9. What techniques can be used to respond to events of concern?
10. What techniques can be used to recover to pre-event capabilities?
11. What techniques can be leveraged to measure the effectiveness of implemented policies and methodologies to iteratively revise security measures?

3 Overview

3.1 Risk Management Overview

Risk management is the ongoing process of identifying, assessing, and responding to risk as related to an organization's mission objectives. To manage risk, organizations should understand any potential impact as well as the likelihood that an event will occur. An organization should also consider statutory and policy requirements that may influence or inform cybersecurity decisions.

The Profile provides a flexible approach for stakeholders to manage risks when interfacing with the satellite bus or payload regardless of the source of the risk, including natural events, malicious actions, and human activities that have unintended consequences. It also provides a starting point from which organizations can customize their risk management approach.

The Profile is intended to be used in conjunction with existing risk management processes to provide additional risk management considerations. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2018, ISO/International Electrotechnical Commission (IEC) 27005, and NIST Special Publication (SP) 800-39 [NIST-SP800-39]. A list of additional resources is included in Appendix C.

3.2 Cybersecurity Framework Overview

Created through collaboration between industry and government, the Cybersecurity Framework [NIST-CSF] provides prioritized, flexible, risk-based, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, and communicate cybersecurity risks.

The Cybersecurity Framework consists of three main components:[2]

1. The *Framework Core* provides a catalog of desired cybersecurity activities and outcomes[3] using common language. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.
2. The *Framework Implementation Tiers* provide context for how an organization views cybersecurity risk management. The Tiers help organizations understand whether they have a functioning and repeatable cybersecurity risk management process and the extent to which cybersecurity risk management is integrated with broader organizational risk management decisions.

[2] Elements of the Cybersecurity Framework – including Core, Implementation Tiers, Profile, Function, Category, and Subcategory – are normally capitalized and will be capitalized throughout this document.

[3] The word "outcomes" is used because the Cybersecurity Framework focuses on the "what" rather than the "how." In other words, the emphasis is on the cybersecurity outcomes that the organization wants to achieve rather than on how they will achieve them. The Informative References provided in Section 4 help organizations with the "how."

3. The *Framework Profiles* are customized to the outcomes of the Core to align with an organization's requirements. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

The Framework Core presents standards, guidelines, and practices within five concurrent and continuous Functions, which are described below:

1. **Identify** – Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational to the effective use of the Cybersecurity Framework, enabling an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and business needs.
2. **Protect** – Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event.
3. **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable the timely discovery of cybersecurity events.
4. **Respond** – Develop and implement the appropriate activities to react to a detected cybersecurity incident. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity incident.
5. **Recover** – Develop and implement appropriate activities to maintain resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations, reduce the impact of a cybersecurity event, and provide insight and guidance for overall improvement.

When considered together, these Functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

The Framework Core then identifies underlying Categories and Subcategories for each Function. The 108 Subcategories are discrete cybersecurity outcomes that are organized into 23 Categories, such as "Asset Management" and "Protective Technology." Figure 3 depicts the basic structure of the Framework Core.

394

395 **Figure 3 - Structure of the Framework Core**

396 The Cybersecurity Framework is outcome-based and focuses on the cybersecurity functions
397 rather than the components. A Cybersecurity Framework Profile is not intended to provide
398 specific implementation guidance. However, a Profile will supply Informative References to
399 existing standards, guidelines, and practices that provide practical guidance to help an
400 organization achieve the desired outcome of each Subcategory. An example of two
401 Subcategories and their Informative References within the Asset Management Category is
402 shown in Figure 4.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5

404 **Figure 4 - Cybersecurity Framework Subcategory Example**

405 A *Cybersecurity Framework Profile* is an assessment of an organization in the context of the
406 Cybersecurity Framework Core. A *"current" Profile* is a review of the Core Subcategories in
407 terms of their applicability and current efficacy from the perspective of the organization. A
408 *"target" Profile* is a set of Subcategories that are selected by an organization as being relevant to
409 achieving a desired cybersecurity state. A gap is identified when a target Subcategory is missing
410 or insufficiently implemented by the current Profile.

411 The Cybersecurity Framework [NIST-CSF] provides additional guidance regarding its purpose
412 and use.

4 Baseline Profile

This section was created by using the Cybersecurity Framework, as described in Section 3.2. The tables summarize the Subcategories within a Category for a Function. The Informative References provide additional guidance.

By design, the Cybersecurity Framework is inherently flexible to accommodate the unique environments and needs of different organizations. Users of this document should understand that deviations between their enterprise and the assumptions made in this Profile will impact the applicability of the Subcategories. ***Therefore, stakeholders are advised to review all of the Subcategories (including those considered not applicable) in the context of their organization.***

4.1 Identify Function

The Identify Function is foundational to the risk assessment process; risk management practitioners should start with the Identify Function. In order to manage risks and assets, they first have to be identified. Consideration of the organization's mission and business objectives, threat environment, assets, and vulnerabilities will have a significant influence on the overall risk management decision and will also impact the other four Functions (i.e., Protect, Detect, Respond, Recover).

The objectives of the Identify Function include:

- Identify the business or operational environment and organization's purpose;
- Identify all assets, including hardware, software, personnel, roles, responsibilities, and the assets' criticality;
- Identify infrastructure that provides ground segment functionality; and
- Identify the current and trending vulnerabilities, threats, and impacts should the threat be realized to assess the risk.

The Identify Function within the Cybersecurity Framework defines six Categories, which are summarized in Table 1: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management. Each of these Categories has at least one Subcategory that applies to the ground segment. However, organizations should review all Subcategories in the Identify Function in case any of them apply to the organization's environment.

442

Table 1 - Baseline Profile for the Identify Function

Subcategory	Applicability to the Ground Segment	References
Identify: Asset Management Category The data, personnel, devices, systems, and facilities that enable the organization to achieve its business objectives are identified and managed in a manner that is consistent with their importance to organizational objectives and the organization's risk strategy. Asset management and prioritization are important factors in other functions and activities, such as contingency planning for future attacks, responding to malware events, emergency responses, and recovery actions. Asset management will assist in prioritizing response and recovery activities.		
ID.AM-1: Physical devices and systems within the organization are inventoried.	Organizations should document and maintain an inventory of the components, to include cloud-based resources, that reflect the current system. Organizations should also consider incorporating a configuration management tool that documents the physical location of all physical components, then verify each component's location and identify its physical interfaces during physical inspections.	[NIST-SP800-53r5] CM-8, CM-9, PM-5 [NIST-SP800-160V1] 2.3
ID.AM-2: Software platforms and applications within the organization are inventoried.	Organizations should document and maintain an inventory of software components, including applications, firmware, and operating systems. The inventory should also include non-traditional components such as virtual machine images and application programming interfaces (APIs). Relevant information, such as licenses and versions, should also be added. The software inventory should be reviewed and updated as defined by the organization.	[NIST-SP800-53r5] CM-8, PM-5 [NIST-SP800-204]
ID.AM-3: Organizational communication and data flows are mapped.	Organizations should identify all connections within and between systems and should document, authorize, and review all connections and interfaces. Connection information may include physical and logical interface characteristics, data characteristics, ports, protocols, addresses, security requirements, and connection purposes. Some components (such as those that directly send commands to the space segment) are normally isolated from other networks. Temporary connections to components for updates, diagnostics, and scanning should be included in the mapping.	[IEC61850-90-4] 10, 14 [NIST-SP800-53r5] AC-4, CA-3, CA-9, PL-8, SA-17
ID.AM-4: External information systems are catalogued.	Typically, connections to external information systems are strictly limited in the ground segment. Organizations should ensure that components that directly interface with space vehicles are securely isolated from external networks but can access necessary data from external sources, such as reachback to the satellite vendor for anomaly resolution support and connections to external databases. How this data is transferred should be catalogued.	[NIST-SP800-53r5] AC-20, PM-5, SA-9

Subcategory	Applicability to the Ground Segment	References
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel and software) are prioritized based on their classification, criticality, and business value.	Organizations should identify and prioritize ground system components, processors, services, and functions based on their classification, criticality, and value in the context of maintaining positive control of the space segment. Organizations should provide adequate staffing with the appropriate training such that support is available in a timely manner (consistent with thresholds defined in the organization's business plan). Stakeholders are advised to use other Functions within the Cybersecurity Framework to inform the identification and prioritization procedures. For example, while testing business continuity procedures, use the findings to identify which resources of the mission were impacted and to what degree, and reprioritize accordingly.	[NIST-SP800-37r2] [NIST-SP800-53r5] AC-20, CP-2, RA-2, RA-9, SA-20, SC-6
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	Organizations should assign cybersecurity roles and responsibilities for the ground systems. The roles and responsibilities for third-party stakeholders and collaborative partners (such as organizations that own or operate payloads that are hosted) are determined on a case-by-case basis.	[NIST-SP800-53r5] CP-2, PM-2, PM-29, PS-7
Identify: Business Environment Category The organization's mission, objectives, stakeholders, and activities are documented, reviewed, and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.		
ID.BE-1: The organization's role in the supply chain is identified and communicated.	Organizations should assess and implement their supply chain risk management policy and procedures with respect to ground segment systems.	[NIST-SP800-53r5] SR-1, SR-3 [NIST-SP800-161]
ID.BE-2: The organization's place in critical infrastructure and its industry sector are identified and communicated.	Depending on the types of payloads or services provided by the satellite, organizations should consider the ground segment's dependencies on and interdependencies with other critical infrastructure segments as part of their broader cyber risk management policy. They should also consider any related regulatory requirements.	[NIST-SP800-53r5] PM-8
ID.BE-3: Priorities for organizational missions, objectives, and activities are established and communicated.	Organizations should consider communicating their priorities, threshold, and objective performance parameters so that potential customers of the satellite services will understand the scope and suitability for their mission.	[NIST-SP800-53r5] PM-11

Subcategory	Applicability to the Ground Segment	References
ID.BE-4: Dependencies and critical functions for the delivery of critical services are established.	Organizations should identify any critical capabilities from other sectors (e.g., power, transportation, communications, etc.) that may impact the mission. The organization's infrastructure – such as network communication architectures, services, protocols, and hardware components – can impact recovery time. Organizations should consider the ground segment's reliance on power supplies and redundant and geographically diverse communication paths.	[NIST-SP800-53r5] CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2
ID.BE-5: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	Resilience requirements for the MOC and PCC are strongly dependent on the space and user segments. The ability for the space segment to function autonomously, the criticality of the services provided by the payload, the system's architecture, and procedural considerations will all define upper and lower bounds on resilience requirements (such as recovery time, periods of outage, etc.).	[IEC61850-90-4] 12.2, 14.2.4 [NIST-SP800-53r5] CP-2, CP-11, RA-9, SA-8, SA-20
Identify: Governance Category The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are documented, reviewed, and inform the management of cybersecurity risk.		
ID.GV-1: Organizational cybersecurity policy is established and communicated.	This subcategory enables the organization to identify key functions and assign areas of responsibility to ensure a comprehensive cybersecurity approach.	[NIST-SP800-53r5] AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	Organizations should define roles and responsibilities between the organization and any third party, such as cloud-based infrastructures or other services. These agreements are typically made in advance. Clearly defined internal roles and responsibilities will facilitate a response in a time of duress. The MOC may require coordination with external partners for space situational awareness and space weather conditions. If the PCC is operated by an external partner, then coordination of the roles and responsibilities between the mission owner and payload operations should be determined in advance on a case-by-case basis.	[NIST-SP800-53r5] PM-1, PM-2, PM-29, PS-7, PS-9

Subcategory	Applicability to the Ground Segment	References
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	The MOC and PCC interface with the bus or payloads – not the data contained – so civil liberties and privacy considerations are generally not applicable, but organizations should review the ground segment and associated services for any relevant regulatory and legal requirements.	[NIST-SP800-53r5] AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1
ID.GV-4: Governance and risk management processes address cybersecurity risks.	Organizations should develop comprehensive risk management strategies that include cybersecurity considerations. For organizations that host payloads, the risk management processes for C2 of the bus may be influenced by changes in the payload mission. Organizations should also review and update their risk management strategy as necessary.	[NIST-SP800-53r5] PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2 [NIST-SP800-160V1] 3.3.8
Identify: Risk Assessment Category The organization documents and reviews the cybersecurity risk to operations (including mission, functions, image, or reputation), assets, and individuals. The ground segment is an important part of the organization's risk assessment process, but attributes such as impact and likelihood must consider the space and user segments. Risk assessments are not normally done by individual segments. Typically, the analysis is performed by a separate group within the organization that considers the entire mission.		
ID.RA-1: Asset vulnerabilities are identified and documented.	Organizations should identify, document, and report vulnerabilities that exist in the ground segment. Vulnerability scanning is normally tested on a representative system to ensure that it is safe and feasible for the operational system. There are alternatives to vulnerability scanning that would be less risky for operational systems, like using information from asset and configuration management technologies to find known vulnerable versions of software and known security misconfigurations. Organizations should test systems frequently and prioritize documenting discovered vulnerabilities. Testing should also occur whenever there have been modifications to the system.	[NIST-SP800-53r5] CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources.	Organizations should have procedures and processes to receive and analyze threat intelligence from a variety of sources.	[CISA-ICS] [DHS-NCCIC] [NIST-SP800-53r5] PM-15, PM-16, RA-10, SI-5 [NIST-SP800-150]

Subcategory	Applicability to the Ground Segment	References
	Commercial entities can use resources such as reports generated by vendors, public interest groups, industry associations and sector-specific organizations (space Information Sharing and Analysis Center [ISAC] for this sector). In some cases, threat intelligence may be received from national sources through appropriate channels.	
ID.RA-3: Threats, both internal and external, are identified and documented.	Organizations should incorporate threat modeling processes to identify and understand existing and future threats to the ground segment. Potential threat modeling categories may include kinetic physical, non-kinetic physical, electronic, and cybersecurity threats. Threat identification and documentation are not limited to malicious attacks or threats to information systems. Organizations also need to consider natural disasters, accidents, etc.	[CCSDS-GREEN] [DIA-SPACE] [NASIC] [NIST-IR8179] [NIST-SP800-37r2] [NIST-SP800-53r5] PM-12, PM-16, RA-3, RA-10, SI-5 [NIST-SP800-154] [NIST-SP800-160V1] 2.3 [RTCA-DO-235] 4-12
ID.RA-4: Potential business impacts and likelihoods are identified.	Organizations should identify any potential impacts based on the results of performing ID.RA-1 through ID.RA-3. Stakeholders should be made aware that this type of analysis is probabilistic and typically presented as a range. Likelihood is impacted by externalities, such as a time of peace versus a time of heightened tensions. For malicious threat agents, likelihood is a function of capability and intent. Assessments should be updated as organizations' knowledge of threat agents' capabilities increase and events occur that may increase the likelihood of attack. The impact analysis should be updated as the organization's business and knowledge evolves.	[NIST-SP800-53r5] CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 [RTCA-DO-235] 2.1, 13
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	The risk determination requires a coordinated effort between threat analysts (for capability and intent of threat agents), system designers (for vulnerability assessment), and the mission owner (for impact). Organizations should reassess risk on a periodic basis, and when there is a substantive change to: • The system's vulnerabilities (such as an equipment upgrade), • A change in the likelihood of threat realization (such as a time of international tension),	[IETF-RFC8915] 3-9 [NIST-SP800-30r1] [NIST-SP800-53r5] CA-2, CA-7, PM-16, PM-28, RA-2, RA-3 [NIST-SP800-160V1] 2.3, 2.4 [RTCA-DO-235] 2.1-2.4, 3, 14

Subcategory	Applicability to the Ground Segment	References
	• A change in the impact should a threat be realized (such as an organization's increased use or dependency on the satellites' payload services), or • As a result of lessons learned from recovery activities.	
ID.RA-6: Risk responses are identified and prioritized.	Organizations should have processes and procedures to identify and prioritize risk responses. Risk responses include activities such as acknowledging and accepting the risk, transferring the risk, mitigating the risk by addressing vulnerabilities through technical or operational means, or eliminating the risk by changing operations.	[NIST-SP800-53r5] CA-5, PM-4, PM-9, PM-28, RA-7
Identify: Risk Management Strategy Category The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. The risk management strategy takes into consideration the risk factors of all three segments (space, ground, and user) as appropriate. This profile concentrates on the inclusion of the ground segment in the risk management strategy.		
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	Organizations should establish risk management processes that detail how the risk management strategy is developed for the organization. Although this profile concentrates on the ground segment, organizations will use the same processes and aspects for the space and user segments, and the final risk management strategy will include all three segments.	[NIST-SP800-53r5] PM-9, PM-28
ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	Organizations should determine the risk tolerance for their ground segment. This risk tolerance will include the MOC and PCC. The organizational risk tolerance of the ground segment can then be used in the risk management of the space and user segments.	[NIST-SP800-53r5] PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	Organizations should determine their risk tolerance related to the ground segment. An organization may determine its risk tolerance across all of the segments that it operates. Risk tolerance will be determined by the entire organization (to include the space and user segment), and the risks of the ground segment should be included in that determination, including the MOC and the PCC.	[NIST-SP800-53r5] PM-8, PM-9, PM-11, RA-9

Subcategory	Applicability to the Ground Segment	References
Identify: Supply Chain Risk Management Category The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.		
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	Due to the nature of the ground segment, some of the equipment used is highly specialized with a limited supply chain. Organizations should consider this specialized nature when determining and managing supply chain risk. Supply chain risk management processes and procedures should also consider the unique delivery of updates and patching necessitated by the constrained external connections of the ground segment. The MOC has constrained external connections and critical components that directly communicate with the space segment and are typically securely isolated from the network.	[NIST-SP800-53r5] PM-30, SA-9, SR-1, SR-2, SR-3, SR-5 [NIST-SP800-161]
ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	Organizations should consider having multiple sources for hardware or software to facilitate line-item replacement by different manufacturers. This measure can avoid supply chain breakage impacts due to the loss of a vendor or poor production lots that delay the delivery of equipment. Use of third-party partners with the ground segment is atypical. Any use of third parties should be limited, and information should be securely isolated from the partner. Organizations should remain informed of current and future regulations related to the acquisition of services (such as buses to accommodate a hosted payload) and devices that may form and transport C2 messages or receive payload acknowledgements or telemetry.	[NIST-SP800-53r5] PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6 [NIST-SP800-161] 2.2, 3
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Organizations should have processes in place to develop and review contracts to ensure that the contracts meet the needs of the ground segment, including regulatory constraints. Considerations may include: 1. Functional requirements; 2. Any relevant and applicable federal law, regulation, or policy; 3. The threat environment; 4. Mission-level goals, criticality, and functions; 5. Security policies; 6. Organizational policies; and 7. Business objectives.	[NDAA] Section 889 [NIST-SP800-53r5] SA-4, SA-9, SR-2, SR-3, SR-5

Subcategory	Applicability to the Ground Segment	References
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.	Organizations should conduct assessments and evaluations in the context of supply chain considerations for the ground segment, such as: 1. The risk of counterfeit systems and components, 2. The development and operational environment of the supplier, 3. The logistics or delivery environment, and 4. Protection measures for sensitive information and data. The organization should consider access paths within the supply chain that might allow adversaries to gain information and introduce hardware, software, or firmware that could cause disruption of the space or ground segment, as well as any dependencies that may exist.	[NIST-SP800-53r5] AU-6, CA-2, CA-7, PS-7, SA-9, SA-11
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	Organizations should include suppliers and third-party providers in recovery planning and testing as appropriate for the ground segment. Scenarios where this may apply include situations where: • PCC and MOC are independent organizations • There is a cloud service provider • An independent organization is leasing ground sites, antennas, etc. Typically, such activities are done in advance of satellite launch, though modifications in these activities may take place throughout the life of the satellite.	[NIST-SP800-53r5] CP-2, CP-4, IR-3, IR-4, IR-8, IR-9

4.2 Protect Function

The Protect Function includes development, implementation, and verification measures to prevent the loss of assurance or functionality within the ground segment. Additionally, the Protect Function enables the response to and recovery from cybersecurity events with planning and preparation activities, while the execution of risk mitigation is addressed in the Response and Recovery Functions.

Space operations use custom software and hardware that were generally not created to be part of a modern, highly interconnected cyber-ecosystem. This can be especially problematic with legacy components that may have been created prior to the development of security best practices or that use obsolete security measures. Where conventional information technology (IT) cybersecurity measures may not be available, the Profile strives to suggest compensating controls. Where practical, this section addresses some of the issues that may result from legacy or repurposed components. Organizations should apply additional consideration to niche

components.

The objectives of the Protect Function include:

- Protecting the systems that format and transmit commands to the required level of assurance;
- Protecting the systems that receive and process telemetry or other data from the satellite; and,
- Should a threat be realized, protecting the ground segment to maintain a sufficient level of operations through verified response and recovery plans and prevent adverse impacts on the space segment.

The Protect Function defines six Categories that are summarized in Table 2: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology. Each of these Categories has at least one Subcategory that applies to the ground segment. However, organizations should review all Subcategories in the Protect Function in case any of them apply to the organization's environment.

Table 2 - Baseline Profile for the Protect Function

Subcategory	Applicability to the Ground Segment	References
Protect: Access Control Category Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices. The extent of the management and the degree of the limitations are consistent with the assessed risk of unauthorized access. In the context of the ground segment, assets may include antennas, receivers, and servers. "Physical access" may include measures to protect RF emanations through means such as directional antennas, beam shaping, the use of access codes within direct-sequence spread spectrum (DSS) implementations, etc. Emergency scenarios will be more thoroughly addressed in the Respond and Recover functions. However, there are important impacts within the Access Control category. Due to the environment in which the ground segment operates, the organization may have to bypass regular access controls in an emergency.		
AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	Organizations should have processes and procedures to manage credentials, including issuance, verification, revocation, and auditing. Organizations should revoke credentials when the authorization of operators, devices, and processes expire or are no longer needed.	[NIST-SP800-53r5] IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12
PR.AC-2: Physical access to assets is managed and protected.	Organizations should define physical access procedures and controls for the ground segment for normal operations, including remote assets. Organizations should establish procedures for physical access in emergency situations that enable effective emergency response in a timely manner.	[NIST-IR8320] [NIST-SP800-53r5] PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9

Subcategory	Applicability to the Ground Segment	References
	Organizations should restrict and manage physical access to antenna fields and operation centers and consider hardware-enabled security for remote physical assets.	
PR.AC-3: Remote access is managed.	Organizations should manage connections to and from the ground segment in accordance with organizational policies and procedures. Organizations should consider securely isolating components that directly communicate with the space segment. This can be done by disconnecting from external networks, privileged access components, and role-based access controls. Traditionally, ground segment isolation was accomplished through air gapping or limited connections. Increasingly, isolation is accomplished via accounts, tenant isolation, and identities when using third-party services. Organizations may permit or require remote access to the ground segment as part of their standard operations. Organizations should assess the risk of remote access or transition to cloud-based services. Remote access could be part of an organization's emergency response. If implemented, organizations should allow limited remote access to a subset of personnel using machines that are directly controlled and maintained by the organization.	[NIST-SP800-53r5] AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Organizations should establish policies, procedures, and processes to manage access permissions and authorizations. These policies and controls should enforce least-privilege principles for access to the ground segment. Organizations can consider having limited access under risk-based adaptive policies that provide access on a limited time or limited privilege basis. Organizations should configure access to components and services such that functionality is limited to performing tasks associated with satellite operations. Organizations should develop mandatory access controls and provide any additional access with discretionary access controls to limit the authorization of an authenticated user. Organizations should consider implementing role-based access control to achieve granular authorization that limits users to assigned tasks and responsibilities. Organizations should define access and authorization controls for normal operations and for emergency situations.	[NIST-SP800-53r5] AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 [NIST-SP800-160V1] Appendix F.1.14

Subcategory	Applicability to the Ground Segment	References
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	Organizations should establish procedures and controls to protect the integrity of ground segment networks. For example, organizations can impact radius for breaches and prevent lateral movement by segmenting access by network, user, device, and application.	[NIST-SP800-53r5] AC-4, AC-10, SC-7, SC-10, SC-20
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	Organizations should verify the identities of users (this can include people, systems, and software) to the appropriate level of assurance prior to issuing credentials. When validating credentials, organizations should consider contextual information, such as geographic location, normal duty hours, task(s) being executed relative to normal tasking, etc.	[ATIS-I-0000070] 2-7 [NIST-IR8014] 4-6 [NIST-SP800-53r5] AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12, PE-2, PS-3
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	Organizations should establish procedures and controls to ensure that users, devices, services, and others are authenticated before allowing connections. The ground segment provides the only communications to the space segment, so preventing unauthenticated communication should be a high priority. Traditionally, the ground segment requires physical access and authentication when initiating a session communicating with the space segment. Organizations should evaluate the risks and implement adequate controls if they are transitioning to more remote operations or cloud-based implementations. Controls like requirements for multi-factor authentication, which provide additional protection, should be considered. Per-transaction authentication may be problematic for communications between the space and ground segments as it can cause unacceptable latency in communications. Therefore, the organization should consider compensating controls for authentication prior to communication with the space segment, such as logins or physical access controls.	[IETF-RFC4082] 2-5 [IETF-RFC7822] 2-4 [NIST-SP800-53r5] AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10
Protect: Awareness and Training Category The organization's personnel and partners are provided cybersecurity awareness education and trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. The awareness and training category is not unique to the satellite industry. The focus is on privileged users who operate, monitor, and maintain equipment that interfaces with the space segment and third-party partners. In the hosted payload scenario, third-party partnerships between the PCC and the MOC vary widely and are coordinated in advance.		
PR.AT-1: All users are informed and trained.	Organizations should provide awareness education and training for all ground segment personnel for the bus and payload.	[NIST-SP800-53r5] AT-2, PM-13, PM-14

Subcategory	Applicability to the Ground Segment	References
PR.AT-2: Privileged users understand their roles and responsibilities.	Organizations should provide more specialized training to ground segment personnel for the bus and payload in accordance with the granularity of the authorization and operation policies.	[NIST-SP800-53r5] AT-3, PM-13 [NIST-SP800-160V1] Appendix E
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	Organizations should establish and have agreement between third-party organizations and the ground segment on the definitions of roles and responsibilities. Throughout the space community, there is a wide range of third-party relationships, such as: • A payload and a host are owned or operated by independent organizations; • The ground segment has a contractual relationship with the space segment for on-orbit anomaly resolution; or • An organization uses cloud-based infrastructure from a cloud service provider for the ground segment.	[NIST-SP800-53r5] AT-3, PS-7, SA-9
PR.AT-4: Senior executives understand their roles and responsibilities.	Organizations should ensure that their senior executives understand their roles and responsibilities. This is especially relevant in emergency scenarios involving the ground segment. In the event of an emergency, senior executives may need to override granular authorization processes implemented in the MOC and PCC. Organizations should train senior executives for these scenarios.	[NIST-SP800-53r5] AT-3, PM-13
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	Organizations should ensure that physical security and cybersecurity personnel in the ground segment understand their roles and responsibilities.	[NIST-SP800-53r5] AT-3, CP-3, IR-2, PM-13

Subcategory	Applicability to the Ground Segment	References
Protect: Data Security Category Information and data are managed to protect the confidentiality, integrity, and availability of commands, responses, or telemetry in a manner that is consistent with the organization's risk strategy. In the context of the ground segment, the focus is on the TT&C uplinks and downlinks. Some of the typical characteristics of these data flows include: • Relatively low bandwidth requirements • Intolerant to latency • Intolerant to jitter • Archiving in accordance with legal requirements or organization policy		
PR.DS-1: Data at rest is protected.	Organizations should implement policies and controls so that data at rest is protected in accordance with risk. Risk is determined, in part, by the sensitivity of the data under consideration. The more sensitive the data, the greater the protection needed. Similarly, the risk should also be informed by how and from where the data is accessed (e.g., if a request originates from unmanaged devices or is from digital media). Organizations should consider controls for data at rest on operational systems, backup systems, and digital media. Such controls can include access control lists, encryption, and physical controls to prevent access. Organizations should also consider storing data separately from the operational system so that the information is retained even if the system is lost.	[GPS-ICD-870] 3.3, 3.3.1 [NIST-SP800-37r2] 3 [NIST-SP800-53r5] MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 [NIST-SP800-175Br1] [NIST-SP800-209]
PR.DS-2: Data in transit is protected.	Organizations should establish a policy and controls to protect data in transit in the ground segment. Command uplinks are typically encrypted and authenticated. Consider measures such as a command count or nonce to protect against replay attacks or spoofing. Organizations should verify that all sessions are encrypted end to end. The RF environment in which the ground segment operates experiences interference, and space assets are subject to a significant free space path loss. Organizations should consider the possible impacts of these aspects on protection measures for data in transit. With the use of RF as the main communication conduit, organizations should consider transmission security measures such as error detection and error correction, as well as bulk link encryption and other transport layer protections.	[IETF-RFC2488] [IETF-RFC2760] [NIST-SP800-53r5] SC-8, SC-11, SC-12 [Rodriguez-Bejarano-2012]

Subcategory	Applicability to the Ground Segment	References
	Organizations should consider measures (e.g., spread spectrum, error detection, error correction, etc.) to mitigate jamming, denial of service, and integrity attacks in accordance with the organization's availability and integrity requirements.	
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	Organizations should establish policies and procedures to manage assets throughout their life cycle. Media sanitization and zeroization of cryptographic variables should be given special consideration.	[NIST-SP800-53r5] CM-8, MP-6, PE-16, PE-20
PR.DS-4: Adequate capacity to ensure availability is maintained.	Organizations should determine what level of availability needs to be maintained and establish the required capacity for their ground segments. Commands, response, and telemetry tend to be low-bandwidth operations, and availability constraints are normally due to RF environmental events. The command link is sensitive to delay and jitter. All services and communications pathways to and from the spacecraft should be examined to ensure that they have adequate capacity to handle peak throughput requirements. If organizations are using service providers, they should consider what capacity exists at the ground station to maintain data rates in case organizations are disconnected from other systems.	[IEC62439-3] 4, 5, Appendix P.2.3, 4.6, 4.8, 4.9, 4.12, 4.13 [NIST-SP800-53r5] AU-4, CP-2, PE-11, SC-5 [NIST-SP800-160V1] Appendix F.4
PR.DS-5: Protections against data leaks are implemented.	Organizations should implement and evaluate protections against data leaks, especially after changes in operating procedures or the adoption of new systems. Within a ground segment, many of these protections can be provided by functions such as authentication, the isolation of information flows, strict access control, and the encryption of data in transit.	[GPS-ICD-240] [NIST-SP800-53r5] AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	Organizations should adopt processes and procedures to provide integrity protection consistent with the architecture, design, and available technologies. For example, implementations could use encryption for command uplinks to provide confidentiality and mitigate replay attacks, digital signatures for authentication to provide a level of information integrity, and supply chain risk management technologies and procedures that provide a level of assurance for software and firmware. Organizations should have processes and procedures in place to protect hardware, firmware, and code from unauthorized access and tampering. Processes should help prevent unauthorized modifications, both inadvertent and intentional, that could circumvent or negate the intended security characteristics.	[GPS-ICD-240] [NASA-NPR7150-2c] [NIST-SP800-53r5] SI-7, SI-10 [NIST-SP800-160V1] 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F [NIST-SP800-161] [NIST-SP800-193] [NIST-SP800-218] PO.3.3, PS.1

Subcategory	Applicability to the Ground Segment	References
	Given the high value of satellites, organizations should consider if additional measures are warranted for any integrity loss that could result in the loss or damage of the space vehicle. These additional controls could include two-person integrity controls for high-risk, high-sensitivity commands.	
PR.DS-7: The development and testing environments are separate from the production environment.	Due to the high value of the space segment and the risk of damage from the ground segment, organizations should not deploy untested software and systems on the production systems of the ground segment. Organizations should consider using a development environment for testing software updates and system modifications. This type of testing can reduce the risk of failure or damage to the production systems. The development and testing environment can employ the use of digital twins. In addition, organizations should consider maintaining a current configuration baseline.	[NIST-SP800-53r5] CM-2 [NIST-SP800-160V1] 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F
PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity.	Controls in this category work in conjunction with other Categories, such as Identify: Asset Management and Identify: Supply Chain Risk Management. Organizations should consider the use of hardware-enabled security, trusted platform modules (TPMs), and anti-tamper controls as defined in FIPS 140-3.	[FIPS140-3] [NIST-IR8320] [NIST-SP800-53r5] SA-10, SI-7 [NIST-SP1800-19] [NIST-SP1800-34]
Protect: Information Protection Processes and Procedures Category Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.		
PR.IP-1: A baseline configuration of information technology/industrial control systems is created, maintained, and incorporates security principles (e.g., concept of least functionality).	Maintaining a baseline configuration is especially important to the ground segment. In most cases, it is not practical to upgrade the space segment, and changes to the configuration of the ground segment can have unforeseen consequences. A secured and maintained configuration baseline can help avoid these consequences. Information assurance requirements and configuration may impact the overall performance of the system, so organizations should verify that the baseline configuration results in a system that meets the baseline performance requirements, such as delay, wander, and jitter tolerances.	[NIST-SP800-53r5] CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 [NIST-SP800-137] Section D [NIST-SP800-160V1] 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G [RTCA-DO-235]

Subcategory	Applicability to the Ground Segment	References
	Organizations should install and configure devices and components per manufacturer instructions using established best practices. They should also understand the limitations of the original equipment being fielded and verify that devices and components are suitable. Organizations should configure the MOC and PCC in a manner such that only essential capabilities are provided to minimize complexity. Reduced complexity can reduce the attack surface and impact recovery time.	
PR.IP-2: A System Development Life Cycle to manage systems is implemented.	Organizations should incorporate and manage security measures throughout the life cycle of components. This should include documenting the requirements, approach, architectures, and assumptions used to minimize risks for systems. Organizations should consider the intended lifetime of systems that are dependent on the ground segment and be aware that systems nearing end of life may have parts/components obsolescence or availability issues.	[NIST-SP800-53r5] SA-3, SA-4, SA-8, SA-10, SA-11 [NIST-SP800-160V1] 3.2.1, Appendix F.3
PR.IP-3: Configuration change control processes are in place.	Organizations should employ configuration change control that is consistent with the software development life cycle to maintain a functioning baseline for the ground segment and its components. Organizations should monitor all changes to validate impacts and integrity and conduct impact analyses prior to deploying a change. Organizations should provide a mechanism so that changes to the firmware and software can be returned to a proper working state.	[NIST-SP800-53r5] CM-3, CM-4, SA-10 [NIST-SP800-137] Section D [NIST-SP800-160V1] 3.3.5, 3.8.3, 3.8.4
PR.IP-4: Backups of information are conducted, maintained, and tested.	Within a ground segment, backup of information is typically provided as part of the implementation of other Subcategories, especially PR.IP-9 and 10. Ground segment organizations typically have one or more redundant facilities that include transmitters, receivers, and servers that are fully backed up and capable of generating commands, processing telemetry, etc.	[NIST-SP800-53r5] CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	The organization should review the physical operating environment to ensure that policies and regulations are met for the ground segment. This could include reviewing emergency lighting, fire protection, and climate controls.	[NIST-SP800-53r5] PE-1
PR.IP-6: Data is destroyed according to policy.	The organization should conduct reviews to ensure that data is destroyed according to policy. This could include reviewing data sanitization procedures and component disposal.	[NIST-SP800-53r5] MP-6, SR-12

Subcategory	Applicability to the Ground Segment	References
PR.IP-7: Protection processes are improved.	The organization does assessments to identify areas for improvement in protection processes for the ground segment. These assessments can include reviewing plans and implementing measures of performance.	[NIST-SP800-53r5] CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6
PR.IP-8: The effectiveness of protection technologies is shared.	The organization shares information on the effectiveness of protection technologies as appropriate. This Subcategory is important for commercial-off-the-shelf (COTS) hardware and software that are implemented in the ground segment. However, the ground segment contains many components that are unique to space operations and may not have relevant information to share outside of other organizations in the space industry. Organizations should consider what might be useful to share within the space industry.	[NIST-SP800-53r5] AC-21, CA-7, CP-2, IR-8, SI-4 [NIST-SP800-150]
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Organizations should develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as provide a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, tests, metrics, contingency roles, personnel assignments, and contact information. Plans should prioritize maintaining essential functions despite system disruption or manipulation, as well as the eventual restoration of normal operations. This is especially relevant to the ground segment. Space assets are high-cost, high-value assets that are inaccessible, have a limited ability to act autonomously, and are reliant on the ground segment. Response and business continuity plans for the ground segment need to be executed in a manner that is consistent with the space segment's ability to operate autonomously and, in the case of a congested orbital slot, to avoid collisions.	[IEC61850-90-12] 5.8, 4.12-4.14 [NIST-SP800-53r5] CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9, PE-17 [NIST-SP800-61r2] [NIST-SP800-160V1] 6.5, 6.6, Appendix F.2
PR.IP-10: Response and recovery plans are tested.	Organizations should assess preparedness by testing incident response and recovery plans to verify effectiveness and for training purposes. Organizations should also consider qualification and periodic testing to assess the response and recovery plans as the satellites lose capabilities due to age or changes to space operations that would significantly impact the performance requirements for the ground segment. Organizations should review the results of testing to determine the efficiency and effectiveness of the plans, as well as a readiness to execute the plans. The results can also be used to inform other Cybersecurity Framework Functions, such as Detect.	[IEC61850-90-4] 14.2.4, 5.4.2.5 [NERC-GridEx] [NIST-SP800-53r5] CP-4, IR-3, PM-14 [NIST-SP800-115]

Subcategory	Applicability to the Ground Segment	References
	The testing and verification of recovery plans should be done in a manner that does not impact operations. Consider the use of digital twins or other test environments (refer to PR.DS-7). The testing of response and recovery plans can validate the command link's availability, integrity, and confidentiality and confirm that it remains within specified tolerances throughout an incident.	
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	Given the high value of space assets and the potential of international incidents, organizations should consider measures such as periodic background checks and screenings for MOC and PCC personnel.	[NIST-SP800-53r5] PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21
PR.IP-12: A vulnerability management plan is developed and implemented.	Organizations should have a plan to address and mitigate identified vulnerabilities for the ground segment. This may be part of a wider vulnerability management plan that covers the entire organization.	[CISA-CIVR-PB] Appendix A [NIST-SP800-53r5] RA-1, RA-3, RA-5, SI-2
Protect: Maintenance Category Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. The ground segment may have to perform maintenance tasks on behalf of space vehicles and should consider that in its maintenance and repair activities.		
PR.MA-1: The maintenance and repair of organizational assets are performed and logged with approved and controlled tools.	Organizations should schedule, perform, record, and review records of maintenance and repairs for the ground segment. As part of that review, organizations should assess the impacts of the maintenance and repair on the MOC and PCC devices and components on the satellite bus and payload operations. The organization should also verify that its performance is within specified tolerances. To facilitate proper maintenance and ensure consistent and valid operations, organizations should make available and require adherence to documentation and artifacts, such as software maintenance procedures, configuration parameters (including default values and ranges), test plans, compliance test result documentation, and other pertinent information.	[NIST-SP800-53r5] MA-1, MA-2, MA-3, MA-5, MA-6

Subcategory	Applicability to the Ground Segment	References
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	Since remote maintenance is especially applicable to the ground segment, organizations should implement procedures to ensure that remote maintenance is performed correctly. The space segment contains high-value assets that are physically inaccessible and mostly receive maintenance through the ground segment. Organizations should consider enhanced protections for remote maintenance in these circumstances, including the enhanced protection of communications, strict access control, and logging actions.	[NIST-SP800-53r5] MA-4 [NIST-SP800-160V1] Appendix F.1.14
Protect: Protective Technology Category Technical security solutions are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements.		
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	The ground segment is responsible for maintaining audit/log records for both the ground and space segments. Due to the spatial environment, there can be significant implications to any incident, whether cyber or physical. Organizations should have logging procedures for: • TT&C data, • Chains of events as required by regulations, and • Any data related to repositioning or on-orbit anomalies. Wherever practical, logging and audit mechanisms should produce data elements in accordance with standard data formats to facilitate parsing and consumption by analytic teams. Organizations should consider maintaining audit logs for extended periods to support forensic analysis. Audit logging should be determined by risk tolerance and tailored by industry best practices.	[NIST-SP800-53r5] AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16 [NIST-SP800-92] [NIST-SP800-160V1] 3.3.2, 3.3.5
PR.PT-2: Removable media is protected, and its use is restricted according to policy.	The use of removable media in the ground segment can be required for purposes such as cryptographic key loading/rotation, software and firmware updates, or other data transfers for air-gapped components. Organizations should have a policy that clearly defines any restrictions on the use of removable media and lays out the safeguards to enforce those restrictions. Such policies are necessary to protect the physical media and maintain a log of its chain of custody.	[NIST-SP800-53r5] MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8

Subcategory	Applicability to the Ground Segment	References
PR. PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Organizations should configure the ground segment system's hardware and software to only provide essential capabilities. Disabled functionality will minimize attack surfaces and facilitate detection.	[NIST-SP800-53r5] AC-3, CM-7
PR.PT-4: Communications and control networks are protected.	The MOC and PCC have high availability and integrity requirements. Organizations should consider the protection of communications and control networks throughout the life cycle. Some controls can only be applied during the architectural phase, while others can be added in the operations or deployment phases. The implementation of some security measures can lead to performance degradation. Organizations should verify that protective measures will not adversely affect overall system performance requirements.	[NIST-CSF] PR.PT-P3 [NIST-SP800-53r5] AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 [NIST-SP800-160V1] Appendix F
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	The duration for which a space vehicle may operate autonomously without communication from the ground segment defines the lower bound of resilience requirements. Stringent resilience requirements may necessitate hot swaps at the MOC and PCC facilities, while cold spares may be sufficient for other organizations. The resilience of other sectors within the critical infrastructure may impact the ground segment. Organizations should consider measures as applicable, such as power backup, redundant communications infrastructure, and alternate service providers. Some organizations use mobile ground sites to provide geographic diversity. Measures should be taken to mitigate attacks that penetrate the ground segment, including holdover capabilities paired with anomaly detection, features to limit performance degradation, and recovery capabilities.	[NIST-SP800-53r5] CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6

4.3 Detect Function

The Detect Function addresses the development and deployment of appropriate activities to monitor for anomalous events and notify users and applications upon their occurrence. The Detect Function is informed by the Identify Function and is enabled by the Protect Function.

The objectives of the Detect Function include:

- Enabling detection through monitoring and consistency checking and
- Establishing a process for deploying detection capabilities and the handling/disposition of detected anomalies and events.

The Detect Function may leverage capabilities such as automation and Security Information and Event Management (SIEM) to assist in detecting previously uncovered threats and minimize false positives. These capabilities involve data parsing, analytics, and the sharing of information. If practical, comply with standards-based solutions for data formatting, message formatting, and message transmission to facilitate interoperability, integration, and sharing.

The Detect Function defines three Categories, all of which have Subcategories that apply to the ground segment to varying degrees, as summarized in Table 3.

Table 3 - Baseline Profile for the Detect Function

Subcategory	Applicability to the Ground Segment	References
Detect: Anomalies and Events Category Anomalous activity is detected, and the potential impact of events is understood.		
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	Organizations should verify that operational performance baselines and expected data flows are captured, developed, and maintained to detect events. Due to the connected nature of the ground and space segments, this baseline may also include the space segment.	[NIST-SP800-53r5] AC-4, CA-3, CM-2, SC-16, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	Organizations should review and analyze detected events within the ground segment to: 1. Forensically understand the characteristics of anomalous events and 2. Maintain authorized operations. Organizations should be able to distinguish between potentially harmful events and normal operations and to predict harm based on early indications and events. When organizations see events that affect space vehicles, they should analyze whether MOC and PCC systems are involved. Organizations should have procedures to preserve raw data, analysis, and characterization to aid in the analysis of future events. Organizations should understand that the ground segment has the responsibility to analyze events on behalf of the space segment.	[NIST-SP800-53r5] AU-6, CA-7, IR-4, RA-5, SI-4 [NIST-SP800-128] [RTCA-DO-235] 2.1

Subcategory	Applicability to the Ground Segment	References
DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	Organizations can use multiple sensors and sources to correlate events, cross-check detected anomalies, and contribute to anomaly detection models and algorithms. Organizations should compile event data across the ground segment using various sources, such as event reports, logs, audit monitoring, network monitoring, physical access monitoring, environmental monitoring, and human-machine interface (HMI) reports. Organizations should consider the inclusion of events from external and shared resources (e.g., open source, industry forums, user groups, etc.).	[NIST-SP800-53r5] AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 [NIST-SP800-160V1] 3.3.7, Appendix G.2, Appendix G.3 [RTCA-DO-235] 1.1
DE.AE-4: The impact of events is determined.	Organizations should have procedures to identify the impact of events on the ground segment. Events (including infrequent events and true anomalies) can have unexpected impacts on connected devices and operations, so organizations should also consider any potential impacts to the space segment.	[NIST-SP800-53r5] CP-2, IR-4, IR-5, IR-8, SI-4
DE.AE-5: Incident alert thresholds are established.	Organizations should establish incident thresholds with an understanding of potential impacts to both the ground segment and the space segment (where indicated). Attributes such as criticality, sensitivity, and tolerance to false positives will vary among stakeholders. Discussions regarding the setting and review of thresholds may need to include external stakeholders. For critical applications, organizations can document error and uncertainty tolerances that serve as detection thresholds. These thresholds can be expressed as a statistical distribution within the confidence levels needed for operations. Organizations should consider and document the required notification or alarm communication time upon nearing and exceeding thresholds. Organizations should review these thresholds periodically.	[NIST-SP800-53r5] IR-4, IR-5, IR-8

Subcategory	Applicability to the Ground Segment	References
Detect: Security Continuous Monitoring Category The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. The granularity of the monitoring and the depth of the analysis are consistent with the findings of the risk assessment (refer to ID.RA-1 through ID.RA-5). In the context of the ground segment, this category covers the interface to the bus or payload, the receivers that process and form the commands, responses and telemetry, the processed telemetry, and the state of health information from the space segment.		
DE.CM-1: The network is monitored to detect potential cybersecurity events.	Organizations should monitor network activity within the ground segment with special attention given to the bus and payload TT&C. System monitoring activities should be heightened when there is an indication of increased risk. Organizations should correlate data from diverse sensors and probes, including using fault detection and exclusion algorithms to automatically detect faults and exclude erroneous sources in the analytics. These actions enable redundancy and consistency checking. Organizations should verify that the monitoring strategy is sufficiently robust to detect space and ground segment behavior anomalies for all identified fault and failure modes. Detection thresholds should be determined from nominal and anomalous historical data for each fault and failure mode. Detection models can leverage correlations between fault modes and minimum detectable limits. Analysis of the correlation engines may be able to determine if some faults can remain undetected. These findings can then be used in the risk management procedures. As RF transmissions are critical to space operations, organizations should have a continuous monitoring program for identifying and responding to interfering and potentially hostile RF emanations. Software and hardware can be integrated into the ground segment to detect and mitigate jamming and spoofing events to preserve data availability and integrity.	[NIST-IR7800] [NIST-SP800-53r5] AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 [RTCA-DO-235] 2.3, 2.5
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	Organizations should monitor physical access to ground segment facilities to detect potential breaches in security. Because of the reliance on the RF environment, organizations should also monitor the RF environment for interfering or potentially hostile emanations. Ground segment equipment – such as antennas and alternate facilities – may be in remote locations, and the near-real-time physical monitoring of remote sites can be challenging. Organizations can consider technologies that generate alerts in real time as well as require periodic physical inspections of remote sites.	[NIST-SP800-53r5] CA-7, PE-6, PE-20

Subcategory	Applicability to the Ground Segment	References
	Other controls that organizations should consider are ones that positively identify people who access these remote areas (e.g., use of biometrics, swipe cards, and PINs).	
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	Organizations should monitor personnel actions for unauthorized or atypical activity. The scope of the monitoring can include elements such as login attributes (e.g., time, physical location, operating system, device, credentials), electronic access control systems, physical access control systems (e.g., sign in/out sheets, logging), and security status monitoring of personnel. Since unauthorized personnel activity at the ground segment can affect both the ground and space segments, organizations should have access and monitoring controls in place for actions that can affect both segments.	[NIST-SP800-53r5] AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected.	Given the importance of least functionality within the ground segment, organizations should have controls to ensure that all code that is not authorized and verified is detected. Due to the SWaP constraints within space vehicles, it may be impractical for the space vehicle to detect malware within itself. Therefore, organizations should consider measures to enable the ground segment to detect malicious code across the space segment (e.g., by interrogating traffic going to/from the satellite for signs of malware).	[NIST-SP800-53r5] SC-44, SI-3, SI-4, SI-8 [NIST-SP800-218]
DE.CM-5: Unauthorized mobile code is detected.	Given the importance of least functionality, organizations should ensure that all mobile code has been approved. This control is especially germane to organizations that have adopted cloud-based infrastructure.	[NIST-SP800-53r5] SC-18, SC-44, SI-4
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Connections to the MOC or PCC are strictly controlled, and in most cases, least privilege principles (e.g., restricted access, limited connectivity, etc.) should be enacted. Organizations that implement third-party suppliers or services, such as cloud-based infrastructures, should monitor and analyze the activity to verify that it is in accordance with predefined agreements (see PR.AT-3). Data flows should be encrypted with independent key management. However, because of the encryption, strong analysis tools like deep packet inspection may not be possible, so data flows can only be superficially monitored. Therefore, these communications may require alternative analytics. Flows that are associated with custom protocols and specifications will be similarly challenging to analyze and may require additional consideration.	[NIST-SP800-53r5] CA-7, PS-7, SA-4, SA-9, SI-4

Subcategory	Applicability to the Ground Segment	References
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	Remote access should also be granted under the principles of least functionality, least privilege, and separation of duties. Organizations should monitor for system discrepancies from inventory and conduct ongoing security status monitoring on ground systems for unauthorized personnel, connections, devices, access points, and software.	[NIST-SP800-53r5] AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed.	Organizations should conduct vulnerability scans on ground systems where safe, feasible, and in a manner that is consistent with industry best practices and the organization's risk tolerance. Organizations should ensure that scanning activities are predefined and do not impact operations. Organizations could also consider ground segment technologies and measures to perform vulnerability scans on the space segment. If practical to do so, organizations may perform the scans on a digital twin or other test system rather than on the space segment itself (see PR.DS-7).	[NIST-SP800-53r5] RA-5 [NIST-SP800-115]
Detect: Detection Processes Category Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. In the context of the ground segment, the processes and procedures related to the information systems, assets, and analytic processes and procedures are maintained, updated, and tested.		
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	All roles – including data collection, analytics, reporting, and notification – are identified, and performance criteria are defined. PCCs responsible for hosted payloads should have an agreement on these roles and responsibilities with the host's MOC.	[NIST-SP800-53r5] CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements.	Organizations should confirm that their detection activities comply with applicable requirements. Organizations with MOCs responsible for hosting third-party payloads should perform detection activities in accordance with predefined agreements for hosted payloads.	[NIST-SP800-53r5] AC-1, AT-1, AU-1, CA-1, CA-2, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1 PE-1, PL-1, PM-1, PM-14, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SI-4, SR-1, SR-9, SR-10
DE.DP-3: Detection processes are tested.	Organizations should validate that event detection processes are operating as intended and within predefined thresholds that include false positives and efficacy of the detection (e.g., false negatives). Detection processes should be revalidated when the ground system is upgraded or modified for the collection of the correct data elements as well as end-to-end testing.	[NIST-SP800-53r5] CA-2, CA-7. PM-14, SI-3, SI-4

Subcategory	Applicability to the Ground Segment	References
	Organizations should periodically test to verify the performance of the detection process against the most current threat profiles and vulnerabilities.	
DE.DP-4: Event detection information is communicated.	Organizations should consider sharing detected information with regional Computer Emergency Response Teams (CERTs) or industry organizations, such as ISACs. MOCs with buses that host (or PCCs that are hosted by an independent organization) may have prearranged information sharing agreements.	[NIST-SP800-53r5] AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved.	Organizations should modify and improve their monitoring strategy as new fault modes are identified. Periodically, organizations should examine their anomaly detection processes and determine if improvements are needed. Tools, techniques, and procedures should be kept current (e.g., updated signatures, intelligence). Organizations can consider the use of technology such as machine learning detection capabilities in tandem with proactive threat hunting based on pre-built queries to reduce false positives, improve detection, and assist in response. Organizations should reevaluate the processes as the space segment ages to ensure sufficient robustness.	[NIST-SP800-53r5] CA-2, CA-7, PL-2, PM-14, RA-5, SI-4

4.4 Respond Function

The activities in the Respond Function support the ability to contain the impact of an incident by developing and implementing appropriate responses to a detected cybersecurity attack or anomalous incident.

The Respond Function actions are triggered by the outputs generated by the Detect Function. The Protect Function enables the Respond Function to execute the proper response to an event according to a predefined plan.

The objectives of the Response Function are to:

- Contain events using a verified response procedure,
- Communicate the occurrence and impact of the event on satellite operations and stakeholders,
- Develop processes to respond to and mitigate new known or anticipated threats or vulnerabilities, and
- Evolve response strategies and plans based on lessons learned.

The Respond Function defines five Categories within the Cybersecurity Framework, as

summarized in Table 4.

Table 4 - Baseline Profile for the Respond Function

Subcategory	Applicability to the Ground Segment	References
Respond: Response Planning Category Response processes and procedures are executed and maintained after detected cybersecurity incidents.		
RS.RP-1: The response plan is executed during or after an incident.	Organizations should execute a response plan during or after a cybersecurity event that impacts space systems in accordance with the predefined threshold. Organizations should document the steps and results of the response plans as they are being executed. It is best to include resilience-level requirements based on criticality and impact categories for incidents. Organizations should update the response plans to address changes to the organization.	[CISA-CIVR-PB] Appendix B [NIST-SP800-53r5] CP-2, CP-10, IR-4, IR-8
Respond: Communications Category Response activities are coordinated with internal and external stakeholders. In the context of the ground segment, external stakeholders may include organizations with payloads that are hosting (or being hosted by) independent organizations.		
RS.CO-1: Personnel know their roles and order of operations when a response is needed.	Organizations should ensure that personnel know, are trained, and have exercised their roles in response to disruptions. Responders should understand recovery time objectives (RTO), recovery point objectives (RPO), restoration priorities, task sequences, and assignment responsibilities for event response programs and processes in a manner that is consistent with business continuity objectives.	[NIST-SP800-34r1] 3.2.1 [NIST-SP800-53r5] CP-2, CP-3, IR-3, IR-8 [NIST-SP800-61r2]
RS.CO-2: Incidents are reported consistent with established criteria.	Organizations should ensure that cybersecurity events that exceed a predetermined threshold are reported in a manner that is consistent with the response plan and will initiate the response plan in a timely manner.	[DHS-GPS-PR] [NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4
RS.CO-3: Information is shared consistent with response plans.	Timely information exchange within organizations improves the overall efficiency of incident response. Organizations should exchange information with external stakeholders in accordance with prearranged agreements and thresholds to ensure that obligations are met (see ID.GV-2 and DE.AE-5).	[FCC-JAMMER] [NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 2.4

Subcategory	Applicability to the Ground Segment	References
	Organizations should coordinate appropriately with law enforcement officials where applicable. Sharing information with consortia focused on space missions or regulatory bodies will enhance space situational awareness.	
RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	If the satellite hosts third-party payloads, incidents that impact satellite bus operations should be reported to the stakeholders in accordance with the response plan and prearranged agreements with the PCC (see ID.GV-4).	[NIST-SP800-53r5] CP-2, IR-4, IR-8, PE-6 [NIST-SP800-61r2] 2.4
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	Suspected intentional interference should be reported to stakeholders through the appropriate channels and procedures. For example, suspected land-based radio frequency interference (RFI) can be reported to NAVCEN and the NASA Aviation Safety Reporting System for aeronautics. When agreed upon between stakeholders, common data formats facilitate information sharing to strengthen the protection of the user community.	[NIST-SP800-53r5] PM-15, SI-5
Respond: Analysis Category Analysis is conducted to verify the efficacy of the response and support recovery activities.		
RS.AN-1: Notifications from detection systems are investigated.	Organizations should investigate cybersecurity-related notifications generated by the anomaly detection systems. The investigation of RFI may involve, and in some cases require, the notification of external agencies. If public safety is impacted, the RFI should be reported to the Federal Communications Commission (FCC) or other authoritative body and, if applicable, to state and local authorities. Commercial owners and operators may report RFI to the Purposeful Interference Response Team (PIRT), which is an interagency organization within the U.S. Government to facilitate U.S. collaboration to attribute and resolve satellite interference.	[CISA-CIVR-PB] 10 [CISA-RFI-BPG] [NIST-SP800-53r5] AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4 [RTCA-DO-235] 14.1.2
RS.AN-2: The impact of the incident is understood.	Within the ground segment, organizations should understand the full implications of a cybersecurity incident based on thorough investigation and analysis results. Organizations should understand impacts that may affect the space segment, third-party stakeholders (in the case of a MOC that hosts third-party payloads), and/or the end-user community.	[CISA-CIVR-PB] 10 [NIST-SP800-53r5] CP-2, IR-4, RA-3 [NIST-SP800-61r2] 3
RS.AN-3: Forensics are performed.	Organizations should conduct forensic analysis on collected cybersecurity event information to determine if there are any residual effects on the system.	[CISA-CIVR-PB] 16 [NIST-SP800-53r5] AU-7, IR-4

Subcategory	Applicability to the Ground Segment	References
	Conducting forensic analysis can aid in the determination of the root cause.	[NIST-SP800-61r2] 3
RS.AN-4: Incidents are categorized consistent with response plans.	Organizations should categorize cybersecurity incidents according to the level of severity and impact consistent with the response plan. Such categorization may include impacts on the space segment.	[NIST-SP800-53r5] CP-2, IR-4, IR-5, IR-8, RA-3 [NIST-SP800-61r2] 2, 3.2
RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, security researchers).	Organizations should establish processes for responding to vulnerabilities disclosed to the organizations. These processes are especially important when the vulnerability affects systems that interface with the space segment.	[DHS-NCCIC] [GPS-ICD-240] 7.6, 7.7 [NIST-SP800-53r5] CA-1, CA-2, PM-4, PM-15, RA-1, RA-7, SI-5, SR-6 [NIST-SP800-61r2] 3, 3.2 [NIST-SP800-160V1] 3.4.9, 3.4.11
Respond: Mitigation Category Activities are performed to contain an event, mitigate its effects, and resolve the incident.		
RS.MI-1: Incidents are contained.	Organizations should contain cybersecurity incidents to minimize impacts on the ground segment. Containment may require transition to alternate sites and the isolation of the primary MOC in accordance with resiliency-level requirements and the business continuity plan for containment. Containment may also involve rapidly zeroizing processing equipment that contain sensitive data. Some organizations have remote assets in vulnerable locations, and operators may need to quickly disable equipment. Organizations should have processes in place to enable security orchestration automated response (SOAR) capabilities to reduce response time for active threats using machine learning.	[CISA-CIVR-PB] 14 [NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 3.4.1
RS.MI-2: Incidents are mitigated.	Once the effects of the incident are contained, organizations should take steps to return the MOC or PCC to a proper working state. These steps may include the resetting, recalibration, and replacement of units. However, these actions should be done in a manner that does not impact forensic efforts. Organizations should apply patches and updates to mitigate the vulnerability if needed.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 3.4

Subcategory	Applicability to the Ground Segment	References
	Organizations should also consider mitigation strategies such as redundancy, diversity, and segmentation to minimize the impacts of disruptions.	
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	When new vulnerabilities are identified, risk assessments (refer to the Identify: Risk Assessment Category) should be updated. Organizations should then mitigate or document acceptable risks.	[NIST-SP800-53r5] CA-2, CA-7, RA-3, RA-5, RA-7 [NIST-SP800-61r2] 3 [RTCA-DO-235] 3.8, 14.1.4, 14.2-14.4
Respond: Improvements Category This category is a post-incident analysis activity that involves other functions within the Cybersecurity Framework. Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities.		
RS.IM-1: Response plans incorporate lessons learned.	Response plans incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing. Organizations should keep plans updated and implement the resulting changes accordingly.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2]
RS.IM-2: Response strategies are updated.	Organizations should: • Enable an update process for the response plan to consider new threats, improved technology, and lessons learned. • Analyze detected event information and incident responses to reassess the impact of future incidents on the organization. If appropriate, update the risk assessment and risk response. • Determine preventative actions for fault modes by reviewing the identification, protection, and detection functions and updating as applicable. • Revise protection, monitoring, detection, response, and recovery capabilities as needed to mitigate newly identified vulnerabilities in a timely manner. Organizations may have automated processes in place to enable SOAR capabilities to reduce response time. Organizations should evaluate and revise these processes as a result of the lessons learned from the incident.	[NIST-SP800-53r5] CP-2, IR-4, IR-8

4.5 Recover Function

The Recover Function develops and implements the appropriate activities to maintain resilience and restore any capabilities or services that were impaired due to a cybersecurity event.

The activities in the Recover Function support timely recovery to normal operations and return the organization back to its proper working state after an incident has occurred. The effectiveness

509 of the Recover Function is dependent on the implementation of the previous Functions –
510 Identify, Protect, Detect, and Respond.

511 The objectives of the Recover Function are to:

512 • Restore the ground segment's services to a proper working state using a verified
513 recovery procedure so that systems dependent on those services can function properly,

514 • Communicate the recovery activities and status of the ground segment services to
515 stakeholders, and

516 • Evolve recovery strategies and plans based on lessons learned.

517 The Recover Function within the Cybersecurity Framework defines three Categories, which are
518 summarized in Table 5.

519 **Table 5 - Baseline Profile for the Recover Function**

Subcategory	Applicability to the Ground Segment	References
Recover: Recovery Planning Category Recovery processes and procedures are executed and maintained to restore systems or assets affected by cybersecurity incidents to a proper working state. Recovery plans are typically a part of the business continuity plan.		
RC.RP-1: The recovery plan is executed during or after a cybersecurity incident.	Organizations should restore the ground segment system within a predefined, acceptable time period from configuration-controlled and integrity-protected information representing a known good state for the components. Organizations should perform system acceptance testing. The recovery plan can include specific actions for the restoration, recalibration, resetting, and test validation of equipment.	[NIST-SP800-34r1] [NIST-SP800-53r5] CP-10, IR-4, IR-8 [NIST-SP800-160V1] 3.4.11, Appendix F.2.6 [NIST-SP800-184]
Recover: Improvements Category Recovery planning and processes are improved by incorporating lessons learned into future activities. In the context of the ground segment, the efficacy of the recovery actions – such as restoring control of the space segment, test plans, user notification, and failover – are evaluated and improved should a similar event occur.		
RC.IM-1: Recovery plans incorporate lessons learned.	Organizations should update the recovery plan to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, operating environment, and deficiencies encountered during plan implementation, execution, and testing.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4
RC.IM-2: Recovery strategies are updated.	Organizations should evaluate the incident's characteristics and impact to determine if the recovery strategy was sufficient or appropriate (i.e., proportional to the impact) and revise the recovery strategy and corresponding plan accordingly.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4, 3.4.1

Subcategory	Applicability to the Ground Segment	References
Recover: Communications Category Restoration activities are coordinated with internal and external parties. In the context of the ground segment, external parties may include partners that host (or are hosting) a third-party payload. Restoration activities can include corrections for anomalies, calibrations, verification, and validation procedures.		
RC.CO-1: Public relations are managed.	This is not applicable to the organization responsible for the technical operations of the ground segment.	[NIST-SP800-34r1] 4 [NIST-SP800-53r5] IR-4 [NIST-SP800-184] 2.4
RC.CO-2: Reputation is repaired after an incident.	This is not applicable to the organization responsible for the technical operations of the ground segment.	[NIST-SP800-53r5] IR-4 [NIST-SP800-184]
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	Organizations should communicate recovery activities to all relevant internal and external stakeholders, executive teams, and management teams.	[NIST-SP800-34r1] [NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-184]

References

[ATIS-I-0000070] Alliance for Telecommunications Industry Solutions (2018) *Context-Aware Identity Management Framework*, ATIS-I-0000070 (ATIS, Washington, DC). Available at https://access.atis.org/apps/group_public/download.php/43565/ATIS-I0000070.pdf

[CCSDS-GREEN] The Consultative Committee for Space Data Systems (CCSDS) (2022) *Security Threats Against Space Missions*, CCSDS 350.1-G-3 (CCSDS, Washington, DC). Available at https://public.ccsds.org/Pubs/350x1g3.pdf

[CISA-CIVR-PB] Cybersecurity and Infrastructure Security Agency (2021) Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. (CISA, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[CISA-ICS] Cybersecurity and Infrastructure Security Agency (2020) *Industrial Control Systems*. (CISA, Washington, DC). Available at https://us-cert.cisa.gov/ics

[CISA-RFI-BPG] Cybersecurity and Infrastructure Security Agency and SAFECOM/National Council of Statewide Interoperability Coordinators (2020) Radio Frequency Interference Best Practices Guidebook. (CISA, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf

[CNSSI-4009] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[DHS-Cyber-Eco] Department of Homeland Security (2011) Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. (DHS, Washington, DC). Available at https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

[DHS-GPS-PR] Department of Homeland Security (2020) *GPS Problem Reporting*. (US Coast Guard, DHS, Washington, DC). Available at https://www.navcen.uscg.gov/?pageName=gpsUserInput

[DHS-NCCIC] Department of Homeland Security (2012) National Cybersecurity & Communications Integration Center (NCCIC) Overview. (DHS, Washington, DC). Available at https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-2012MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf

[DHS-RCF] Department of Homeland Security (2020) Resilient PNT Conformance Framework. (DHS, Washington, DC). Available at https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf

[DIA-Space] Defense Intelligence Agency (2019) Challenges to Security in Space. (DIA, Washington, DC). Available at https://apps.dtic.mil/sti/pdfs/AD1082341.pdf

[FCC-Jammer] Federal Communications Commission (2020) *Jammer Enforcement*. (FCC, Washington DC). Available at https://www.fcc.gov/general/jammer-enforcement

[FIPS140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[GPS-ICD-240] SAIC (GPS Systems Engineering & Integration [SE&I]) (2019) Navstar GPS Control Segment to User Support Community Interfaces, Global Positioning System Interface Control Document ICD-GPS-240C. (Air Force Space Command, Department of Homeland Security and the U.S. Coast Guard, Washington, DC). Available at https://www.gps.gov/technical/icwg/ICD-GPS-240C.pdf

[GPS-ICD-870] SAIC (GPS SE&I) (2020) NAVSTAR Next Generation GPS Control Segment (OCX) to User Support Community Interface, Global Positioning System Interface Control Document ICD-GPS-870E. (Air Force Space Command, Department of Homeland Security, Department of Transportation, Federal Aviation Administration, and the U.S. Coast Guard, Washington, DC). Available at https://www.gps.gov/technical/icwg/ICD-GPS-870E.pdf

[IEC61850-90-4] International Electrotechnical Commission (2020) *IEC TR 61850-90-4:2020 Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/64801

[IEC61850-90-12] International Electrotechnical Commission (2020) *IEC TR 61850-90-12:2020 Communication networks and systems for power utility automation - Part 90-12: Wide area network engineering guidelines.* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/63706

[IEC62439-3] International Electrotechnical Commission (2021) *IEC 62439-3 Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/64423

[IETF-RFC2488] Allman M, Glover D, Sanchez L (1999) Enhancing TCP Over Satellite Channels using Standard Mechanisms, (Internet Engineering Task Force (IETF) Network Working Group), IETF Best Current Practice (BCP) 28, IETF Request for Comments (RFC) 2488. https://doi.org/10.17487/RFC2488

[IETF-RFC2760] Allman M, Dawkins S, Glover D, Griner J, Tran D, Henderson T, Heidemann J, Touch J, Kruse H, Ostermann S, Scott K, Semke J (2000) Ongoing TCP Research Related to Satellites. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 2760. https://doi.org/10.17487/RFC2760

[IETF-RFC4082] Perrig A, Song D, Canetti R, Tygar JD, Briscoe B (2005) Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 4082. https://doi.org/10.17487/RFC4082

[IETF-RFC7822] Mizrahi T, Mayer D (2016) Network Time Protocol Version 4 (NTPv4) Extension Fields. (Internet Engineering Task Force), IETF Request for Comments (RFC) 7822. https://doi.org/10.17487/RFC7822

[IETF-RFC8915] Franke D, Sibold D, Teichel K, Dansarie M, Sundblad R (2020) Network Time Security for the Network Time Protocol. (Internet Engineering Task Force), IETF RFC 8915. https://doi.org/10.17487/RFC8915

[ITU-T-G.810] International Telecommunications Union Telecommunications Standardization Sector (1996) ITU-T G.810, *Definitions and Terminology for Synchronization Networks* (ITU-T, Geneva, Switzerland), Corrigendum 1, Nov. 2001. Available at https://www.itu.int/rec/T-REC-G.810/en

[NASA-smallsat] Small Spacecraft Systems Virtual Institute (2021) State-of-the-Art Small Spacecraft Technology, NASA/TP—20210021263. (Ames Research Center, NASA, Moffett Field, CA). Available at https://www.nasa.gov/sites/default/files/atoms/files/soa_2021.pdf

[NASA-NPR7150-2c] NASA (2019) NASA Procedural Requirements: NASA Software Engineering Requirements, NPR 7150.2C. Available at https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=7150&s=2B

[NASIC] National Air and Space Intelligence Center (2019) Competing in Space. (NASIC, Dayton, OH). Available at https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-FNV711-0002.PDF

[NCS-2018] The White House (2018) National Cyber Strategy of the United States of America. (The White House, Washington, DC). Available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[NDAA] Department of Defense, General Services Administration, and National Aeronautics and Space Administration (2019) Interim Rule Issued by DoD, GSA, and NASA. (DoD, GSA, and NASA, Washington, DC). Available at https://www.acquisition.gov/FAR-Case-2019009/889_Part_B

[NERC-CIP-008-6] North American Electric Reliability Corporation (2020) *CIP-008-6 – Cyber Security – Incident Reporting and Response Planning.* Available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

[NERC-GridEx] North American Electric Reliability Corporation (2020) *GridEx.* Available at https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

[NIST-CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST-IR7800] Waltermire D, Halbardier A, Humenansky A, Mell P (2012) Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7800 (Draft). Available at https://csrc.nist.gov/CSRC/media/Publications/nistir/7800/draft/documents/Draft-NISTIR-7800.pdf

[NIST-IR8014] Hastings NE, Franklin JM (2015) Considerations for Identity Management in Public Safety Mobile Networks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8014. https://doi.org/10.6028/NIST.IR.8014

[NIST-IR8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

[NIST-IR8270] Scholl M (2022) Introduction to Cybersecurity for Commercial Satellite Operations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8270 (2nd Draft). https://doi.org/10.6028/NIST.IR.8270-draft2

[NIST-IR8320] Bartock M, Souppaya M, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra A, Banks D, Jordan M, Pendarakis D, Rao JR, Romness P, Scarfone K (2022) Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8320. https://doi.org/10.6028/NIST.IR.8320-draft2

[NIST-IR8323] Bartock MJ, Lightman S, Li-Baboud Y, McCarthy J, Reczek K, Brule J, Northrip D, Scholz A, Suloway T (2021) Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8323. https://doi.org/10.6028/NIST.IR.8323

[NIST-SP800-30r1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[NIST-SP800-34r1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[NIST-SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[NIST-SP800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[NIST-SP800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[NIST-SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[NIST-SP800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[NIST-SP800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[NIST-SP800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[NIST-SP800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[NIST-SP800-145] Mell PM, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

[NIST-SP800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[NIST-SP800-154] Souppaya M, Scarfone K (2016) Guide to Data-Centric System Threat Modeling. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-154 (Draft). Available at https://csrc.nist.gov/publications/detail/sp/800-154/draft

[NIST-SP800-160V1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[NIST-SP800-161] Boyens J, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. http://doi.org/10.6028/NIST.SP.800-161

[NIST-SP800-175Br1] Barker EB (2020) Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-175B, Rev. 1. https://doi.org/10.6028/NIST.SP.800-175Br1

[NIST-SP800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[NIST-SP800-193] Regenscheid AR (2018) Platform Firmware Resiliency Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-193. https://doi.org/10.6028/NIST.SP.800-193

[NIST-SP800-204] Chandramouli R (2019) Security Strategies for Microservices-based Application Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-204. https://doi.org/10.6028/NIST.SP.800-204

[NIST-SP800-209] Chandramouli R, Pinhas D (2020) Security Guidelines for Storage Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-209. https://doi.org/10.6028/NIST.SP.800-209

[NIST-SP800-218] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

[NIST-SP1800-19] Bartock M, Souppaya M, Dodson D, Carroll D, Masten R, Scinta G, Massis P, Prafullchandra H, Malnar J, Singh H, Ghandi R, Storey L, Yeluri R, Shea T, Dalton M, Weber R, Scarfone K, Phoenix C, Dukes A, Haskins J, Swarts B (2022) Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-19. Available at https://csrc.nist.gov/publications/detail/sp/1800-19/draft

[NIST-SP1800-34] Diamond T, Grayson N, Polk W, Regenscheid A, Souppaya M, Brown C, Deane C, Scarfone K (2021) Validating the Integrity of Computing Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-34 (Preliminary Draft). Available at https://csrc.nist.gov/publications/detail/sp/1800-34/draft

[NIST-T&F-Glossary] NIST Physical Measurement Laboratory, Time and Frequency Division (2020) Time and Frequency Glossary from A to Z. Available at https://www.nist.gov/pml/time-and-frequency-division/popular-links/time-frequency-z

[PPD-21] Presidential Policy Directive 21 (PPD-21) (2013) Presidential Policy Directive -- Critical Infrastructure Security and Resilience. (The White House, Washington, DC). Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[Rodriguez-Bejarano-2012] Rodriguez Bejarano JM, Yun A, De La Cuesta B (2012) “Security in IP satellite networks: COMSEC and TRANSEC integration aspects.” 2012 6th Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC), pp. 281-288. Available at https://ieeexplore.ieee.org/document/6333089

[RTCA-DO-235] Radio Technical Commission for Aeronautics (2008) *RTCA DO-235A Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band*. (RTCA, Washington, DC). Available at https://standards.globalspec.com/std/1090607/RTCA%20DO-235

[SPD-5] Space Policy Directive 5 (SPD-5) (2020) Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems. (The White House, Washington, DC), September 4, 2020. Available at https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

[USG-FRP] Department of Defense, Department of Homeland Security, and Department of Transportation (2019) 2019 Federal Radionavigation Plan (Department of Transportation, Washington DC). Available at https://www.transportation.gov/pnt/radionavigation-systems-planning

Appendix A—Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

API	Application Programming Interface
ASMS	Advanced Satellite Multimedia Systems Conference
ATIS	Alliance for Telecommunications Industry Solutions
BCP	Best Current Practice
C2	Command and Control
CCSDS	The Consultative Committee for Space Data Systems
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMSAT	Communications Satellite
COMSEC	Communications Security
COTS	Commercial Off the Shelf
C&S	Control and Status
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DoD	Department of Defense
DSSS	Direct-Sequence Spread Spectrum
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
GPS	Global Positioning System
GPS SE&I	Global Positioning System Systems Engineering & Integration
GSA	General Services Administration
HMI	Human-Machine Interface
HSR	High-Availability Seamless Redundancy
IaaS	Infrastructure as a Service

IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISAC	Information Sharing and Analysis Center
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
ITU-T	International Telecommunication Union International Telecommunications Standardization Sector
MOC	Mission Operations Center
NASA	National Aeronautics and Space Administration
NASIC	National Air and Space Intelligence Center
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NTPv4	Network Time Protocol Version 4
PCC	Payload Control Center
PIN	Personal Identification Number
PIRT	Purposeful Interference Response Team
PNT	Positioning, Navigation, and Timing
PPD	Presidential Policy Directive
PRP	Parallel Redundancy Protocol
RF	Radio Frequency
RFC	Request for Comments
RFI	Radio Frequency Interference
RMF	Risk Management Framework
RPO	Recovery Point Objectives
RTCA	Radio Technical Commission for Aeronautics

RTO	Recovery Time Objectives
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automated Response
SP	Special Publication
SPD	Space Policy Directive
SPSC	Signal Processing for Space Communications Workshop
SSDF	Secure Software Development Framework
SWaP	Size, Weight, and Power
TCP	Transmission Control Protocol
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TPI	Two-Person Integrity
TPM	Trusted Platform Module
TRANSEC	Transmission Security
TT&C	Telemetry, Tracking, and Command
U.S.	United States
USG	United States Government

Appendix B—Glossary

Selected terms used in this document are defined below.

Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [CNSSI-4009]

Bus: The primary spacecraft structure containing power, temperature control, and directional thrusters of the satellite that provides locations for the payloads. [NASA-smallsat]

Calibration: A comparison between a device under test and an established standard, such as UTC (NIST). When the calibration is finished, it should be possible to state the estimated time offset and/or frequency offset of the device under test with respect to the standard, as well as the measurement uncertainty. Calibrations can be absolute or relative. Absolute calibrations are not biased by the calibration reference and would, therefore, be more reproducible. However, absolute calibrations can be more complex to determine. The bias in relative calibrations would be consistent if all of the devices in the system are calibrated against the same calibration reference. Calibrations may also be performed relative to other devices without reference to an absolute standard. Relative calibrations are generally simpler to perform than absolute calibrations. [NIST-T&F-Glossary, Adapted]

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [NIST-SP800-145]

Communications Security (COMSEC): A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. [CNSSI-4009]

Component: A hardware, software, or firmware part or element of a larger system with well-defined inputs and outputs and a specific function. [NIST-SP800-160V1, Adapted] [DHS-RCF, Adapted]

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [FIPS200]

Cyber Ecosystem: The aggregation and interactions of a variety of diverse participants (such as private firms, non-profits, governments, individuals, and processes) and cyber devices (computers, software, and communications technologies). [DHS-Cyber-Eco, Adapted]

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. For example, PNT data is generated by cyber systems. Protection of the devices and systems used to generate PNT data

should be considered part of cybersecurity. [NIST-SP800-53r5]

Integrity: A measure of the trust that can be placed in the correctness of the information supplied by a PNT service provider. Integrity includes the ability of the system to provide timely warnings to users when the PNT data should not be used. [USG-FRP]

Interference (electromagnetic): Any electromagnetic disturbance that interrupts, obstructs, degrades, or otherwise limits the performance of user equipment. [USG-FRP, Appendix E]

Jitter: The short-term variations of the significant instants of a timing signal from their ideal positions in time (where short-term implies that these variations are of frequency greater than or equal to 10 Hz). [ITU-T-G.810]

Mission Operations Center (MOC): A facility that provides C2 for the satellite bus, receives TT&C from the satellite, and requests and retrieves data as necessary.

Mobile Code: Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. [CNSSI-4009]

Payload: Elements of the spacecraft that provide (commercial, scientific, or other) services to end-users. [NASA-smallsat, Adapted]

Payload Control Center (PCC): A facility that provides C2 for satellite payloads.

Proper Working State: A condition in which the device or system contains no compromised internal components or data fields (e.g., data stored to memory) and from which the device or system can recognize and process valid input signals and output valid PNT solutions. An initial pre-deployment configuration is a basic example. The accuracy of the immediate PNT solution is not specified in this definition, as it will depend on the specifics of the device or system's performance and the degradation allowed by different resilience levels. [DHS-RCF]

Reliability: The probability of performing a specified function without failure under given conditions for a specified period of time. [USG-FRP]

Remote Access: Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network. [NIST-SP800-53r5]

Resilience: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. [PPD-21]

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST-SP800-37r2]

Risk Assessment: The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets,

individuals, other organizations, and the Nation resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST-SP800-30r1]

Risk Management: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, and includes (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time. [NIST-SP800-39]

Risk Management Framework: A disciplined and structured process that integrates information security and risk management activities into the system development life cycle. [NIST-SP800-37r2]

Secure: To reduce the risks of intrusions and attacks as well as the effects of natural or human-caused disasters on critical infrastructure by physical means or defensive cyber measures. [PPD-21]

Two-Person Integrity (TPI): A system of storage and handling designed to prohibit individual access to certain material by requiring the presence of at least two authorized persons for the task to be performed. [CNSSI-4009, Adapted]

Transmission Security (TRANSEC): Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. Note: TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated. [CNSSI-4009]

Threat: Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, or denial of service. [NIST-SP800-53r5]

Validation: Confirmation (through the provision of strong, sound, and objective evidence and demonstration) that requirements for a specific intended use or application have been fulfilled and that the system, while in use, fulfills its mission or business objectives while providing adequate protection for stakeholder and mission or business assets, minimizing or containing asset loss and associated consequences, and achieving its intended use in its intended operational environment with the desired level of trustworthiness. [NIST-SP800-160V1, Adapted]

Verification: The process of producing objective evidence that sufficiently demonstrates that the system satisfies its security requirements and security characteristics with the level of assurance that applies to the system. [NIST-SP800-160V1, Adapted]

633 **Vulnerability**: A weakness in an information system, system security procedures, internal
634 controls, or implementation that could be exploited or triggered by a threat source. [NIST-
635 SP800-30r1]

Appendix C—Additional Resources

Aerospace Report No. TOR-2016-01797 Ground Segment Systems Engineering Handbook. August 1, 2016. Available through The Aerospace Corporation, El Segundo, CA 90245.

Buenneke R, Abramson R (2006). Best Practices of Commercial Satellite Communications Infrastructure. Available at https://arc.aiaa.org/doi/10.2514/6.2006-5386

Communications Security, Reliability and Interoperability Council VII (2020) Final Report - Risks to 5g from Legacy Vulnerabilities and Best Practices for Mitigation. (Working Group 2: Managing Security Risk in the Transition to 5, CSRIC, Washington, DC). Available at https://www.fcc.gov/file/18918/download

CTIA (2019) Protecting America's Next-Generation Networks (CTIA, Washington, DC). Available at https://api.ctia.org/wp-content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf

Department of Defense. (2015) DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle. (DOD, Washington, DC). Available at https://www.dau.edu/tools/Lists/DAUTools/Attachments/37/DoD%20-%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf

Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. Available at https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf

International Organization for Standardization (2018) ISO 31000:2018 – Risk management – Guidelines (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/65694.html

International Organization for Standardization/International Electrotechnical Commission (2018) ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/75281.html