Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date July 25, 2023

Original Release Date February 25, 2022

Superseding Document

Status	Final
Series/Number	NIST IR 8270
Title	Introduction to Cybersecurity for Commercial Satellite Operations
Publication Date	July 2023
DOI	https://doi.org/10.6028/NIST.IR.8270
CSRC URL	https://csrc.nist.gov/pubs/ir/8270/final
Additional Information	

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Draft (2nd) NISTIR 8270

Introduction to Cybersecurity for Commercial Satellite Operations

Matthew Scholl
Theresa Suloway

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8270-draft2

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

Draft (2nd) NISTIR 8270

Introduction to Cybersecurity for Commercial Satellite Operations

Matthew Scholl
Computer Security Division
Information Technology Laboratory

Theresa Suloway
The MITRE Corporation
McLean, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8270-draft2

February 2022

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

National Institute of Standards and Technology
James K. Oltoff, Performing the Non-Executive 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 8270
49 pages (February 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8270-draft2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: February 25, 2022 – April 8, 2022

Submit comments on this publication to: DraftIR8270Comments@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 is a newly emerging commercial critical infrastructure sector that is no longer the domain of only national government authorities. Space is an inherently risky environment in which to operate, so cybersecurity risks involving commercial space – including those affecting commercial satellite vehicles – need to be understood and managed alongside other types of risks to ensure safe and successful operations. This report provides a general introduction to cybersecurity risk management for the commercial satellite industry as they seek to start managing cybersecurity risks in space. This document is by no means comprehensive in terms of addressing all of the cybersecurity risks to commercial satellite infrastructure, nor does it explore risks to satellite vehicles, which may be introduced through the implementation of cybersecurity controls. The intent is to present basic concepts, generate discussions, and provide sample references for additional information on pertinent cybersecurity risk management models.

Keywords

commercial space satellite operations; cybersecurity; cybersecurity risk management; risk management.

Acknowledgments

The authors wish to thank all contributors to this publication, especially Karen Scarfone and Greg Witte for their technical contributions, Scott Kordella for his tireless assistance, and Isabel Van Wyk for her outstanding technical editing.

Audience

The primary audience for this publication includes chief information officers (CIOs), chief technology officers (CTOs), and risk officers of organizations who are using or plan to use commercial satellite operations and are new to cybersecurity risk management for these operations.

Trademark Information

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: DraftIR8270Comments@nist.gov

Executive Summary

As stated in the September 2018 United States National Cyber Strategy, the U.S. Government considers unfettered access to and freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. Space Policy Directive 5 (SPD-5) was released in 2020 to address the need for cybersecurity in space systems and directed federal agencies to work with non-government space operators to define and establish cybersecurity-informed norms for space systems. This profile is part of NIST's effort to support SPD-5 and its goals for securing space.

Cyber-related threats to space assets (e.g., commercial satellites) and supporting infrastructure pose increasing risk to this economic promise and commercial space emerging markets. Commercial satellite operations occur in an inherently risky environment. Physical risks to these operations are generally quantifiable and have the most likely potential to adversely impact the businesses that operate commercial satellites, usually in low-earth orbit. While this is the primary risk consideration for satellite operations, continued growth in this new commercial infrastructure allows for opportunities to address cybersecurity risks along with other risk elements.[1]

Methods for the creation, maintenance, and implementation of a cybersecurity program for many of the commercial and international markets include products in national and international standard-setting organizations (SSOs), as well as the use of risk management guidance from the National Institute of Standards and Technology (NIST). NIST risk management guidance includes specific technical references, cybersecurity control catalogues, the IT Risk Management Framework, and the Cybersecurity Framework (CSF).

The intent of this document is to introduce the CSF to commercial space businesses. This includes describing a specific method for applying the CSF to a small portion of commercial satellite operations (e.g., a small sensing satellite), creating an example CSF set of desired security outcomes based on missions and anticipated threats, and describing an abstracted set of cybersecurity outcomes, requirements, and suggested cybersecurity controls.

NIST asks the commercial satellite operations community to use this document as an informative reference to assist in managing cybersecurity risks and to consider how cybersecurity requirements might coexist within space vehicle system requirements. The example requirements listed in this document could be used to create an initial baseline. However, NIST recommends that organizations use this document in coordination with the set of NIST references and applicable SSO materials to create cybersecurity outcomes, requirements, and controls customized to support an organization's particular business needs and address its individual threat models.

[1] These can include but are not limited to physical risks, EMI/EMC, financial risks, and supplier and customer risks.

This report focuses on uncrewed commercial space vehicles that will not dock with human-occupied spacecraft.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

The concept of a commercial space sector has been evolving for some time. In 2007, the U.S. Leadership in Space Commerce Strategic Plan stated,

> From television and data communications, to personal navigation, to internet-based satellite imagery, space commerce has enabled countless new economic benefits for our nation. In addition, the expansion of the global market for commercial space capabilities has generated robust worldwide competition. [3]

The White House National Space Policy stated this in 2010:

> The term “commercial,” for the purposes of this policy, refers to space goods, services, or activities provided by private sector enterprises that bear a reasonable portion of the investment risk and responsibility for the activity, operate in accordance with typical market-based incentives for controlling cost and optimizing return on investment, and have the legal capacity to offer these goods or services to existing or potential nongovernmental customers. [4]

Today, space continues to be an evolving commercial sector that is no longer the domain of only national government authorities. The commercial uses of space for research and development, material sciences, communication, and sensing are growing in size, scale, and importance for the future of the U.S. economy. Space is an inherently risky environment in which to operate, so cybersecurity risks involving commercial space need to be understood and managed alongside other types of risks to ensure safe and successful operations.

1.1 Purpose and Scope

This report provides a general introduction to cybersecurity risk management for the commercial space commerce industry. This document does not apply to federally acquired and operated systems, which are regulated by other authorities. This document is by no means comprehensive in terms of addressing all cybersecurity risks to commercial space infrastructure, nor does it explore how cybersecurity solutions might introduce risk to a space vehicle. The intent is to introduce basic concepts, generate discussions, clear confusion, and provide references for additional information on pertinent cybersecurity risk management concepts. ***This report focuses on uncrewed commercial space vehicles that will not dock with human-occupied spacecraft.***

The* Cybersecurity Policy For Space Systems Used to Support National Security Missions *(CNSSP-12) governs the acquisition of national security space systems. The CSF is non-regulatory, and the scope applies to commercial entities that operate space vehicles and payloads that are not owned, operated, controlled, or leased by the U.S. Government.

1.2 Report Structure

This report is organized into the following sections and appendices:

- Section 2 provides a notional, conceptual, high-level architectural view of commercial satellite operations.
- Section 3 describes the steps of the Cybersecurity Framework.
- Section 4 provides a notional example of how a satellite organization might apply the Cybersecurity Framework steps to their space vehicles.
- Appendix A provides examples of regulations that may be relevant to commercial satellite operations.
- Appendix B lists the acronyms used in this report.
- Appendix C list the glossary terms used in this report.

2 Conceptual High-Level Architecture of Satellite Operations

This section provides a notional, conceptual, high-level architectural view of commercial, uncrewed space operations. This view can be helpful in understanding, assigning, and managing cybersecurity requirements and risks associated with different owners and operators of different parts of the architectures. This architecture can be under the sole control of one system owner or shared among numerous public, commercial, and private owners.

Once in operation, space vehicles share an ecosystem that has no national and few natural boundaries and where safety is a communal concern. For the purposes of this paper and to facilitate subsequent discussions in setting, expressing, or meeting cybersecurity requirements, NIST notionally defines the scope of a commercial space operations architecture to include the following:

2.1 Space Architecture Segments

2.1.1 Space Segment:

The space vehicle or satellite consists of the platform and one or more payloads. The bus consists of the components of the vehicle associated with the "flying of the satellite," such as power, structure, attitude control system, processing and command control, and telemetry. The spacecraft can carry many specialized payloads to conduct missions, including remote sensing and communications. The bus and the payload generally combine to form the satellite.

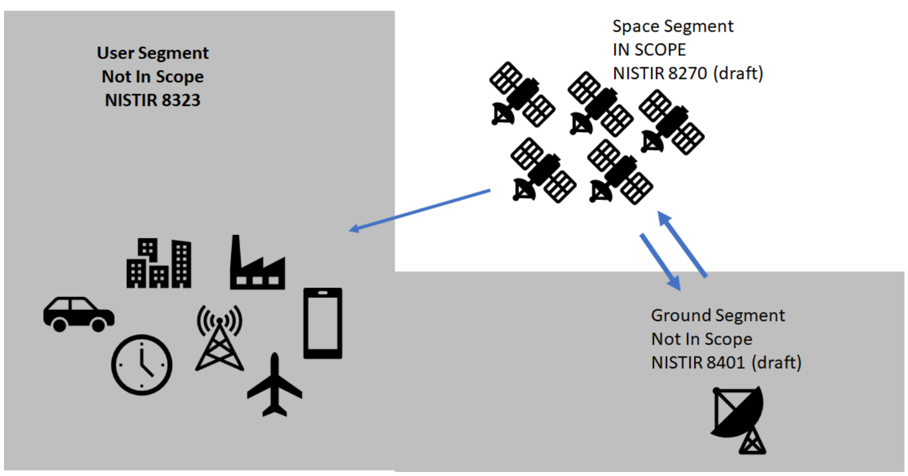


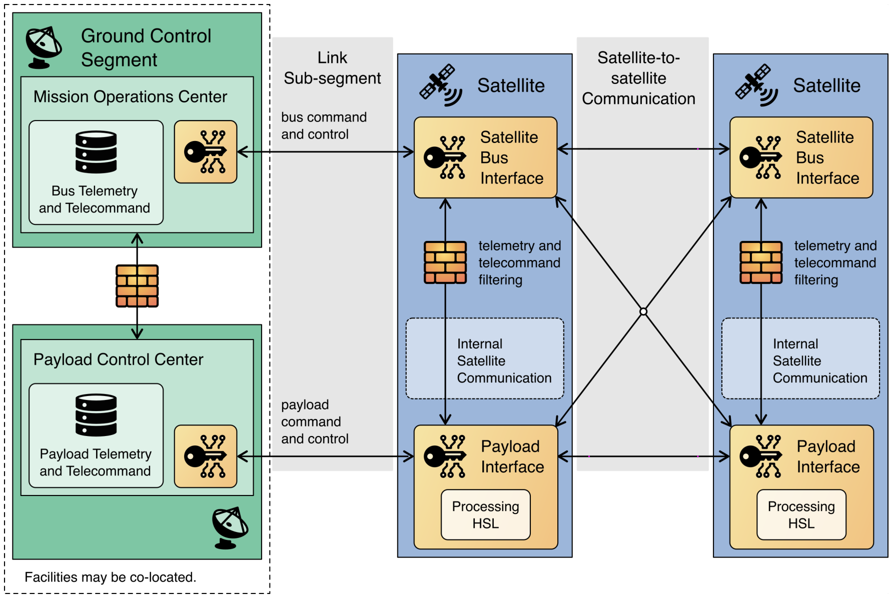
Figure 1 reflects major parts of the conceptual, high-level architecture of satellite operations. This architecture is for uncrewed spacecraft and does not include cybersecurity requirements for human space systems, human spacecraft, or systems that will dock with human systems and/or lunar landers.

2.1.2 Key Considerations and Communications:

Link sub-segment: *Command and control* are the signaling operations sent to the satellite to conduct a mission function, perform diagnostics, reset the state of the equipment, send updates, and/or activate the propulsion systems of the vehicle. Command and control operations are generated on the ground and can be transmitted to the vehicle in several ways. The commands may be sent via a fiber link to a remote ground station, which then transmits the commands via a direct radio frequency (RF) or optical link to the satellite from the ground. The second method uses a set of space relays, where the original commands are sent from the ground via RF or optical to a relay satellite and then transmitted via RF or optical to the target satellite. Finally, mobile devices and technologies not associated with a specific ground operations location, such as intra-vehicle communications, can be used to deliver commands to a satellite or its payload.

Internal Satellite Cybersecurity sub-segment: *Internal vehicle cybersecurity* refers to the cybersecurity capabilities of the satellite vehicle itself, including its ability to protect itself against cybersecurity threats, detect threat actions, respond to cybersecurity attacks, and recover when necessary. These capabilities should be designed as part of security development and integrated early in the system life cycle. Often, internal vehicle cybersecurity is the primary responsibility of small commercial satellite owners and operators, and much of the rest of the architecture is outsourced to external suppliers and providers. Internal vehicle cybersecurity is a feature owned by a satellite in the space segment.

Satellite-to-Satellite Communications sub-segment: Communications between operational satellites for mission functions – such as command and control, networking of compute capabilities, redundancy of operations and mission functions, tracking, and communications – are known as *inter-vehicle communications*. Therefore, the integrity, availability, and confidentiality of these communications are critical. Satellite-to-satellite communications is a capability of a satellite in the space segment and can be for both docked systems as well as space stations, which are composed of separate operational vehicles.



2.1.3 Other Space Architecture Segments

Ground segment: *Ground operations* are terrestrial-based activities that can be automated or conducted by human operators. They often include some or all of the space operations (i.e., station keeping and payload commanding) and can be co-located with launch facilities or at a separate set of facilities. Ground operations can be outsourced in whole or in part. Even at launch, the payload operator may not be collocated with the launch facility.

User segment: These are consumers, such as GPS receivers, satellite phone users, satellite TV receivers, vehicles, 5G users, industrial systems, mobile devices, or aircraft.

2.2 Spacecraft Vehicle Life Cycle Phases

The space vehicle will experience different phases of operations, each of which may have unique risks that need to be addressed. This document focuses on the operations phase of the satellite life cycle.

2.2.1 Operational Phase

Operations – Sensing, Information Processing, Data Acquisition, and Communication: The satellite conducts a mission operation that involves some function or combination of functions for sensing, information processing, data acquisition, and communication. These are functional requirements directly related to the business mission of the satellite and are conducted by the satellite and/or its payloads.

2.2.2 Other Phases

Design/Development: Is it important to have robust software and hardware design processes where developers add in security and perform proper security testing. Manufactures and companies should be aware of the long lifetime of some spacecraft and build in flexibility to address cyber threats over the lifetime of the vehicle. Specific attention should be placed on the cryptographic modules that may potentially allow for upgrades for post-quantum cryptography. Current operationally deployed systems should also consider using compensating controls to achieve outcomes if the legacy technologies are insufficient.

Assembly: Spacecraft components are procured from across the world and brought together to allow the spacecraft to perform various missions. This step should include tests to validate the functions of components and software, including cybersecurity functionality. The hardware, firmware, and software supply chain is, therefore, a critical component of cybersecurity. Once vehicles are launched, the ability to modify hardware is limited, if not impossible. Hardware implants or vulnerabilities are difficult to mitigate and can have a foundational impact on cybersecurity. However, software on a space vehicle can often be patched or modified from the ground. To deter or minimize supply chain attacks, organizations should understand the security and privacy policies of their suppliers and communicate their requirements to their suppliers and their capabilities to their customers. The profile can be a tool to help manage the supply chain, and the importance of the acquisition process cannot be stressed enough (e.g., using trusted vendors, designing/embedding required security).

Prelaunch: This is a critical time for the vehicle during which operators will test RF links and utilize an umbilical cord to the launch vehicle for diagnostics and telemetry. It is important for operators to understand the connectivity and access that the various satellite health and status monitoring systems have during prelaunch and to ensure the cybersecurity of the test environment. This phase also includes transit to the launch facility from the factory and storage at the launch facility before launch –activities that should be controlled for physical access to the vehicle.

Launch: *Launch* is the phase of space commerce that entails moving the space system to its operational environment (e.g., from a pad, rack, ramp, or other device or installation). Launch can include launch devices and installations, fuel operations and storage, and launch safety and destruct systems. Launch can have significant overlap with ground operations, and the two are often combined. However, due to the current cost, complexity, and safety concerns associated with launch, it is often outsourced for small commercial satellites.

On-orbit checkout: Once the satellite is placed into orbit, the satellite must beacon and establish a link to the ground command and control system. The satellite typically undergoes several checks to ensure that the systems have survived launch and are operational. The satellite will then enter operational status. Another critical aspect during this time is that command and control of the satellite transfers from the development organization to the operating organization. This phase of the satellite mission should remain a focus from a cybersecurity perspective due to the change in custody and the visibility of these events, which can potentially provide opportunities for malicious actors.

Decommissioning: The decommissioning of a commercial satellite is a high-risk endeavor with requirements for the post-mission disposition of satellites. General good practices include maintaining control of orbital debris released during normal operations, minimizing debris generated by accidental explosions, and ensuring the post-mission disposal of space structures, either by re-entry and burn up in Earth's atmosphere or by moving the structure to the graveyard orbit. Decommissioning other areas of the space operations architecture can include the need to handle and dispose of sensitive materials, intellectual property, and hazardous materials.

The cybersecurity risks of decommissioning should consider appropriate confidentiality, integrity, and availability considerations, as well as related physical threats to commercial satellite systems once decommissioned. Industry practices – such as following ISO standards for decommissioning, international treaty obligations, and domestic regulations – should also be considered.

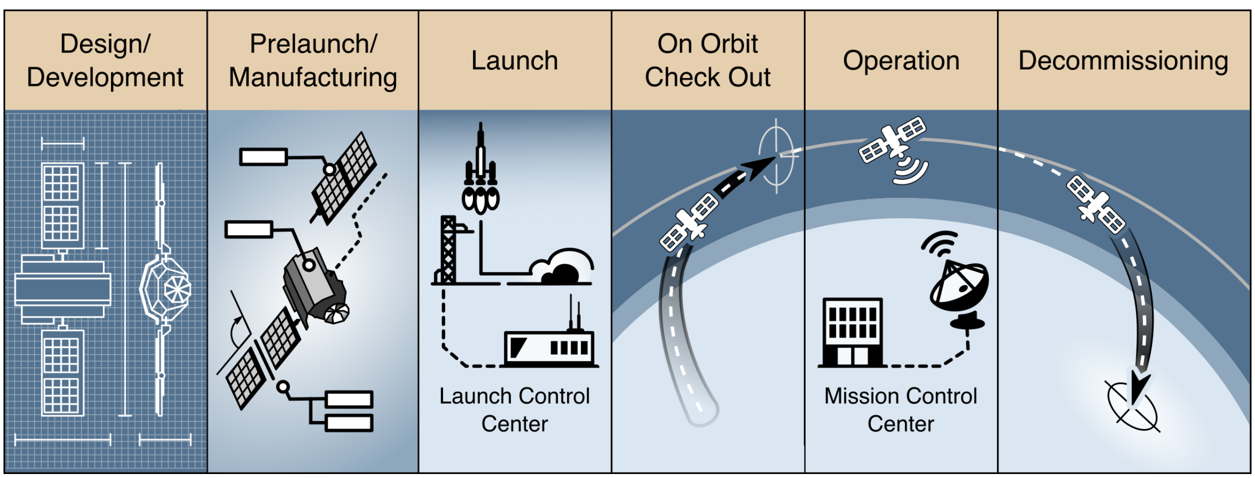
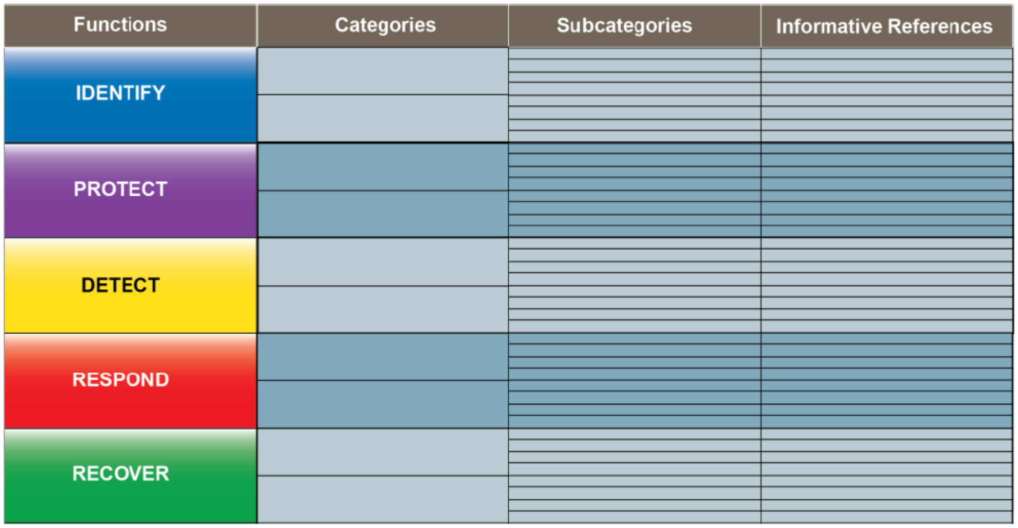


Figure 3. Phases of Operations

3 An Introduction to the Cybersecurity Framework

The Cybersecurity Framework was developed in reponse to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The framework is based on a risk management approach to cybersecurity that can be tailored to various industries. It provides a common terminology and methodology that can be implemented by organizations based on their resources and business needs. The Cybersecurity Framework consists of five functions: identify, protect, detect, respond, and recover. The functions are shown in a circullar format to communicate to the user that cybersecurty is an iterative and continuous process that enables an organization to navigate the changing landscape of cybersecurity risks. Figure 4 shows a visual representation of the CSF and its functions.

In addition to the five primary functions of the Cybersecurity Framework, there are categories and subcategories that express cybersecurity outcomes and informative references to assist in the implementation of controls that can achieve those outcomes.



To help explain the context of the categories, subcategories, and informative references, an example of the first row of *Identify* with the category "asset management" is provided in Figure 6. Each category has associated subcategories, which describe specific outcomes. The last column of information includes references for that particular outcome that cite applicable NIST and SSO publications.

The following section will highlight specific NIST 800-53, Revision 4 and Revision 5, controls that map to the subcategories for the notional scenario.

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 business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS 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
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS 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 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

What is a profile?

A profile is a set of the subcategories from the framework that are selected by an organization to represent either their current cybersecurity state (i.e., current profile) or their desired cybersecurity state (i.e., target profile). The gap analysis between a current and target profile can help an organization develop an action plan to enhance their cybersecurity posture.

4 Creating a Cybersecurity Program for Space Operations

The application of high-level processes from the Cybersecurity Framework may help satellite operators with the creation and maintenance of a cybersecurity program. While the overall process is applicable to all parts of commercial space architectures and phases of operation, this document also provides a notional example of applying the CSF to generating cybersecurity requirements for the satellite during sensing, information processing, data acquisition, and communication to illustrate how these steps are used and to derive example cybersecurity outcomes, requirements, and controls for this specific use.

4.1 Using the Cybersecurity Framework to Develop a Profile

The Cybersecurity Framework can be used to develop a profile that helps organizations communicate their cybersecurity posture and organize cybersecurity-related tasks and activities. The Framework profile can be used to communicate cybersecurity requirements to suppliers and to manage how risk is mitigated, managed, transferred, or accepted when outsourcing one or more aspects of space operations. Commercial space operations can be hybrid modes with few organizations owning or controlling all parts. Therefore, communicating clear expectations, capabilities, and requirements across the different owners of the space operations scope is critical to understanding and managing cybersecurity risks. Notably, the risk to an organization is impacted by changes in that organization's reliance on the assets, an adversary's capability, and an adversary's intent. Effective risk management requires the steps presented in this section to be visited and revisited on a regular basis.

Step 1: Establish Scope and Priorities. It is most effective to address cybersecurity in the earliest stages of building the components of the space architecture and embedding risk-reducing measures that meet organizational mission and business objectives into the design and supply chain. However, many commercial satellite operators have already deployed several generations of their vehicles, and many parts of an architecture are in use.

For companies that have already begun deployment, a current cybersecurity profile should be created to describe what cybersecurity outcomes are being achieved. A target profile can be created to describe the outcomes needed to meet the cybersecurity risk management goals of the organization. A gap analysis of the differences between the current profile and the target profile provides information that the organization can use to make decisions regarding cybersecurity.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for mission and business needs, the organization identifies related systems, assets, regulatory requirements,[2] and its overall risk approach. The organization then works to identify threats and vulnerabilities applicable to those systems and assets.

[2] Some examples of regulatory requirements can be found in Appendix A.

Step 3: Create a Current Profile. This step allows the organization to understand their current cybersecurity posture. An organization can assess how it is currently implementing the CSF functions by creating a Current Profile – a list of subcategory activities that are currently being implemented within the organization.

Step 4: Conduct a Risk Assessment. This initial assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment, identifies emerging risks, and uses cyber threat information from internal and external sources to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

Step 5: Create a Target Profile. The organization creates a Target Profile by selecting the subcategories that support the organization's desired cybersecurity outcomes. Each organization will have a unique risk posture, which will result in a unique set of subcategories.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to identify potential gaps. When paired with a threat, a risk assessment can be conducted to determine an overall risk rating. This will allow organizations to create a prioritized action plan to address those gaps.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps. The Framework is an iterative process that must be repeated at regular intervals, when the impact to the organization changes, or when the cyberthreat landscape changes. Regularly scheduled reviews of the security profile, gap reassessment, updated action plans, and completed action plans should be conducted at least every two years and/or after relevant cybersecurity incidents or discoveries in the industry.

4.2 Case Study Example

This section provides a short example walk-through using the Cybersecurity Framework steps for a notional low-Earth orbit (LEO) "small satellite vehicle," which represents only one portion of larger space operations. The same process[3] can be applied to the other areas of space operations, if needed. In this notional example, a Framework Profile is created to address the core cybersecurity areas below:

- **Identify** assets, threats to those assets, vulnerabilities to those assets, threat models, and regulatory requirements.
- **Protect** assets using outcomes that are then traced to controls and standards.
- **Detect** cybersecurity incidents that result from a risk exposure where an attack has exploited a vulnerability and the realization of threats as they materialize.

[3] It is important to note that the CSF is not prescriptive about how the steps should be applied, and this use case is intended for use as one of many possible methods.

- **Respond** to those incidents..
- **Recover** from those incidents.

4.2.1 Scenario Background

This scenario describes a small company that manufactures and operates a small satellite. The satellite is for commercial use and is only under NOAA regulation[4] for licensing commercial imagery satellites. Initially, this company is focusing on the satellite (platform and payload).

For Step 1 – The notional use case is scoped to just the following aspects of Figure 1: the satellite vehicle itself; internal satellite communication cybersecurity (the interaction and interfaces to components within the vehicle); what the satellite receives, consumes, and produces to outside entities; Command and Control; and Sensing, Information Processing, Data Acquisition and Communication. The notional company only owns and controls the satellite vehicle part of the operations. They will use its generated target profile to express cybersecurity requirements for their vehicle and to compare products and services offered for other areas of space operations that are hybrid and/or outsourced.

For Step 2 – The organization's business leaders identify relevant regulatory requirements as well as critical systems and critical data, and they model potential high-level threats and vulnerabilities to assets (and their potential impacts). The organization defines its critical systems as those with a direct impact on the satellite itself and their business model, which acquires "data over a geographic area." Organizational leadership determines that the business and mission-critical systems are:

- Communications technologies
- Guidance control
- Sensor systems

The organization then generates a high-level cybersecurity risk model that can help identify its most severe cybersecurity vulnerabilities, the threat events that are most likely to occur, and events that could have the highest negative impact on the business. This analysis is less rigid than the detailed risk evaluation that occurs in Step 4 and is intended to spur discussion regarding the types of risk events that might have some impact on the organization. The resulting risk understanding helps shape the Current State Profile described in Step 3.

A list of the potential threats and their business impacts is then generated (see Table 1).

[4] See Licensing | nesdis (noaa.gov).

Table 1. Mapping of cybersecurity potential threats to business impacts

	Cybersecurity potential threats	***Business Impacts***
1	Intentional jamming and spoofing of sensor data	Communications technologies Guidance control Sensor systems
2	Interception and theft of sensor data	Communications technologies
3	Intentional corruption of sensor systems	Sensor systems
4	Denial-of-service attack of sensor	Communications technologies
5	Intentional jamming and spoofing of guidance control	Guidance control
6	Hijacking and unauthorized commands to guidance control	Guidance control
7	Malicious code injection	Communications technologies Sensor systems
8	Denial-of-service attack of guidance	Guidance control

To mitigate these high-impact, high-probability events, a set of needed cybersecurity outcomes is generated. These are, in effect, the inverse of the threat models to the critical systems and are placed in the terms used in the core of the CSF where they are most appropriate for the outcomes. For example:

- *Identify/Protect/Detect/Respond/Recover* from jamming, spoofing, and data interception of communication technologies.
- *Protect/Detect/Respond/Recover Guidance Control* from unauthorized access, unauthorized commands, and unauthorized jamming.
- *Protect/Detect/Respond/Recover* from spoofing, interception, and the corruption of sensor data.
- *Protect/Detect/Respond/Recover Satellite Operations* from malicious code attacks.
- *Protect/Detect/Respond/Recover* communication technologies, sensors, and guidance controls from denial-of-service attacks.

Regulations and other requirements for each component of operations, specifically for the sensing satellite vehicle, are identified and used to generate outcomes that are added to the above list when needed. These are then tagged to identify their sources as regulatory and to ensure that any needed records are generated and maintained on the implementation of these requirements.

Currently, many federal agencies hold oversight over and requirements in different elements of space operations. These are the primary inputs for identifying initial cybersecurity requirements for space commerce systems. Some examples of relevant regulations are described in Appendix A.

<u>For Step 3</u> – Assume that the current cybersecurity program is driven solely by regulatory requirements. In the example use case, these are the NOAA requirements for the Licensing of Private Remote Sensing Space Systems. The organization will need to assure and state that:

> The methods applicant will use to ensure the integrity of its operations, including plans for: Positive control of the remote sensing space system and relevant operations centers and stations; denial of unauthorized access to data transmissions to or from the remote sensing space system; and restriction of collection and/or distribution of unenhanced data from specific areas at the request of the U.S. Government.[5]

The organization documents the policies, processes, and technologies that are in place, especially those related to the high-level cybersecurity risk issues described in Step 2. The organization should walk through all of the subcategories outlined in the Cybersecurity Framework and select those that are currently in practice. The list of subcategories being addressed forms the Current Profile (Table 2).

For the purposes of this example, the company has found that they are currently implementing the following, which will serve as their "Current Profile."

Table 2. Current Profile

Function	Subcategory	Informative Reference	
		SP 800-53, Rev 4	SP 800-53, Rev 5
Protect	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	IA-8	IA-8

[5] See https://www.nesdis.noaa.gov/CRSRA/licenseHome.html.

Function	Subcategory	Informative Reference SP 800-53, Rev 4	SP 800-53, Rev 5
	PR.AC-4: Access permissions and authorizations are managed to incorporate the principles of least privilege and separation of duties.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24	AC-1, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24
	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).	IA-1, IA-2, IA-3, IA-5, IA-9, IA-10, IA-11	IA-1, IA-2, IA-3, IA-5, IA-9, IA-10, IA-11
	PR.DS-1: Data at rest is protected.	SC-28	SC-28
	PR.DS-2: Data in transit is protected.	SC-8	SC-8
	PR.DS-4: An adequate capacity to ensure availability is maintained.	CP-2, SC-5	CP-2, SC-5
	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7	SI-7, SI-10
	PR.IP-12: A vulnerability management plan is developed and implemented.	RA-1, RA-3, RA-5, SI-2	RA-1, RA-3, RA-5, SI-2
	PR.PT-5: Mechanisms (e.g., fail-safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	PL-8, SC-6	PE-11, PL-8, SC-6
Detect	DE.AE-3: Event data is collected and correlated from multiple sources and sensors.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	DE.CM-1: The network is monitored to detect potential cybersecurity events.	SC-5	AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-4: Malicious code is detected.	SI-3	SI-4

Function	Subcategory	Informative Reference SP 800-53, Rev 4	SP 800-53, Rev 5
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, SI-4	AU-12, CA-7, CM-3, CM-8, SI-4

For Step 4 – The organization prioritizes and validates the needed cybersecurity outcomes from Step 3 and uses them to inform the specific technical cybersecurity controls to be selected to meet those outcomes.

The organization considers the costs of cybersecurity mitigation and the potential risks addressed in light of each subcategory recorded in the Current State Profile. The team consults various authorities at the Department of Homeland Security and the Department of Defense to better understand potential threats to space-based network operations. The organization joins a local Information Sharing and Analysis Center (ISAC) so that company representatives will have a venue for sharing and receiving prioritized information regarding known risks as the threat and technology landscapes evolve.

The organization applies the principles described in NIST SP 800-30, *Guide for Conducting Risk Assessments*, to set a scale for likelihood and impact and to prioritize outcomes and controls that can manage the risks with the most negative impacts and/or that are most cost-effective for their risk management results. The results of this notional risk assessment are presented in Table 3. Supported by this information, the organization is then prepared to determine the outcomes that will achieve the desired risk posture in a cost-effective way.

Table 3. Notional Risk Assessment Example

	Cybersecurity Potential Threats	***Business Impacts***	***Severity***	***Likelihood***
1	Intentional jamming and spoofing of sensor data	Loss of data assets for customers	Moderate	Moderate, based on availability of jamming equipment.
2	Interception and theft of sensor data	Loss of markets and customers	High	Moderate, based on availability of receiver equipment
3	Intentional corruption of sensor system	Loss of satellite vehicle or loss of data	Critical	Moderate
4	Denial-of-service attack of sensor	Loss of data and/or loss of service	Moderate	Moderate

	Cybersecurity Potential Threats	*Business Impacts*	*Severity*	*Likelihood*
5	Intentional jamming and spoofing of guidance control	Loss of satellite vehicle	Moderate	Moderate
6	Hijacking and unauthorized commands to guidance control	Loss of satellite vehicle	Critical	Critical
7	Malicious code injection	Loss of satellite vehicle, data corruption, and data loss	Critical	Moderate
8	Denial-of-service attack of guidance	Loss of data and/or loss of guidance	Moderate	Moderate

For Step 5 – The organization creates the following Target Profile to express its desired satellite vehicle cybersecurity requirements. Table 4 maps threats identified in Step 2 to CSF subcategories. These subcategories map to specific SP 800-53 technical controls as found in the informative references section of the Framework.[6] An ordinal count is made for the amount of individual subcategories and threat-pairing that a control might address. This will further assist in establishing priorities and helping with investment decisions. For example, one cybersecurity control might be effective in achieving many of the outcomes sought. This information can assist in understanding priorities as well as mitigations that might need stronger monitoring, detection, and recovery capabilities.

The creation of this mapping builds a list of CSF subcategories and associated informative references that can be used to express the specific technical requirements of the SP 800-53 control. The selection of the subcategories results in Table 5, which is the Target Profile. These include NIST references and those from other sources, such as Standards Development Organizations (SDOs), the Committee on National Security Systems Instruction (CNSSI) 1200, and others that are relevant to the organization.

[6] SP 800-53, Revision 4 and Revision 5 are given in this example.

607 **Table 4. Selection of subcategories to cybersecurity potential threats**

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional corruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
Identify	ID.AM-1								
	ID.AM-2								
	ID.AM-3								
	ID.AM-4								
	ID.AM-5								
	ID.AM-6								
	ID.BE-1								
	ID.BE-2								
	ID.BE-3								
	ID.BE-4								
	ID.BE-5								
	ID.GV-1								
	ID.GV-2								
	ID.GV-3								
	ID.GV-4								
	ID.RA-1								
	ID.RA-2								

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional coruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
	ID.RA-3								
	ID.RA-4								
	ID.RA-5								
	ID.RA-6								
	ID.RM-1								
	ID.RM-2								
	ID.RM-3								
	ID.SC-1								
	ID.SC-2								
	ID.SC-3								
	ID.SC-4								
	ID.SC-5								
Protect	PR.AC-1								
	PR.AC-2								
	PR.AC-3								
	PR.AC-4								
	PR.AC-5								

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional corruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
	PR.AC-6								
	PR.AC-7								
	PR.AT-1								
	PR.AT-2								
	PR.AT-3								
	PR.AT-4								
	PR.AT-5								
	PR.DS-1								
	PR.DS-2								
	PR.DS-3								
	PR.DS-4								
	PR.DS-5								
	PR.DS-6								
	PR.DS-7								
	PR.DS-8								
	PR.IP-1								
	PR.IP-2								

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional corruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
	PR.IP-3								
	PR.IP-4								
	PR.IP-5								
	PR.IP-6								
	PR.IP-7								
	PR.IP-8								
	PR.IP-9								
	PR.IP-10								
	PR.IP-11								
	PR.IP-12								
	PR.MA-1								
	PR.MA-2								
	PR.PT-1								
	PR.PT-2								
	PR.PT-3								
	PR.PT-4								
	PR.PT-5								

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional corruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
Detect	DE.AE-1								
	DE.AE-2								
	DE.AE-3								
	DE.AE-4								
	DE.AE-5								
	DE.CM-1								
	DE.CM-2								
	DE.CM-3								
	DE.CM-4								
	DE.CM-5								
	DE.CM-6								
	DE.CM-7								
	DE.CM-8								
	DE.DP-1								
	DE.DP-2								
	DE.DP-3								
	DE.DP-4								

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional corruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
	DE.DP-5								
Respond	RS.RP-1								
	RS.CO-1								
	RS.CO-2								
	RS.CO-3								
	RS.CO-4								
	RS.CO-5								
	RS.AN-1								
	RS.AN-2								
	RS.AN-3								
	RS.AN-4								
	RS.AN-5								
	RS.MI-1								
	RS.MI-2								
	RS.MI-3								
	RS.IM-1								
	RS.IM-2								

Functions	Subcategories	1 Intentional jamming and spoofing of sensor data	2 Interception and theft of sensor data	3 Intentional corruption of sensor systems	4 Denial-of-service attack of sensor	5 Intentional jamming and spoofing of guidance control	6 Hijacking and unauthorized commands to guidance control	7 Malicious code injection	8 Denial-of-service attack of guidance
Recover	RC.RP-1								
	RC.IM-1								
	RC.IM-2								
	RC.CO-1								
	RC.CO-2								
	RC.CO-3								

Table 5: Target Profile

Functions	Subcategories	Informative Reference SP 800-53 Rev 4	SP 800-53 Rev 5
Identify	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15
	ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources.	SI-5, PM-15, PM-16	SI-5, PM-15, PM-16, RA-10

Functions	Subcategories	Informative Reference SP 800-53 Rev 4	Informative Reference SP 800-53 Rev 5
	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.	AU-6, PS-7, SA-9	AU-6, CA-2, CA-7, PS-7, SA-9, SA-11
Protect	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	IA-8	IA-8
	PR.AC-3: Remote access is managed.	AC-1, AC-19, SC-15	AC-1, AC-19, SC-15
	PR.AC-4: Access permissions and authorizations are managed to incorporate the principles of least privilege and separation of duties.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24	AC-1, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	AC-16, IA-1, IA-2, IA-4, IA-5, IA-12, PE-2, PS-3	AC-16, IA-1, IA-2, IA-4, IA-5, 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).	IA-1, IA-2, IA-3, IA-5, IA-9, IA-10, IA-11	IA-1, IA-2, IA-3, IA-5, IA-9, IA-10, IA-11
	PR.DS-1: Data-at-rest is protected.	SC-28	SC-28
	PR.DS-2: Data-in-transit is protected.	SC-8	SC-8
	PR.DS-4: An adequate capacity to ensure availability is maintained.	CP-2, SC-5	CP-2, PE-11, SC-5

Functions	Subcategories	Informative Reference SP 800-53 Rev 4	Informative Reference SP 800-53 Rev 5
	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7	SI-7, SI-10
	PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity.	SI-7	SI-7
	PR.IP-1: A baseline configuration of information technology/industrial control systems that incorporates security principles (e.g. concept of least functionality) is created and maintained.	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
	PR.IP-3: Configuration change control processes are in place.	CM-3, 4, 10	CM-3, 4, SA-10
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	PS 2,3,4,5,6,7, CM-7	CM-7
	PR.IP-12: A vulnerability management plan is developed and implemented.	RA-1, RA-3, RA-5, SI-2	RA-1, RA-3, RA-5, SI-2
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	AU Family	AU1, 2, 3, 6, 7, 12, 13, 14, 16
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	AC-3, 8, 9,19	AC-3, CM-7

Functions	Subcategories	Informative Reference SP 800-53 Rev 4	Informative Reference SP 800-53 Rev 5
	PR.PT-4: Communications and control networks are protected.	SC-32, AC-4, AC-17, SC-7	AC-12, AC-17, CP-8, SC-5, SC-7, SC-10, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47
	PR.PT-5: Mechanisms (e.g., fail-safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	PL-8, SC-6	PE-11, PL-8, SC-6
Detect	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	DE.CM-1: The network is monitored to detect potential cybersecurity events.	SC-5	AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-4: Malicious code is detected.	SI-3	SI-4
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, SI-4	AU-12, CA-7, CM-3, CM-8, SI-4
	DE.DP-4: Event detection information is communicated.	AU-6, CA-2, CA-7, RA-5, SI-4	AU-6, CA-2, CA-7, RA-5, SI-4
Respond	RS.CO-5: Voluntary information-sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	SI-5, PM-15	SI-5, PM-15
	RS.AN-1: Notifications from detection systems are investigated.	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4
	RS.AN-3: Forensics are performed.	AU-7, IR-4	AU-7, IR-4

Functions	Subcategories	Informative Reference SP 800-53 Rev 4	Informative Reference SP 800-53 Rev 5
	RS.MI-1: Incidents are contained.	IR-4	IR-4, CP-2, IR-8
Recover	RC.RP-1: The recovery plan is executed during or after a cybersecurity incident.	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8,
	RC.IM-2: Recovery strategies are updated.	CP-2, IR-4, IR-8	CP-2, IR-4, IR-8

For Step 6 – The organization compares the desired cybersecurity state (as reflected in Table 5) and the current cybersecurity state (as reflected in Table 2). The organization determines a new cybersecurity baseline, and each row in the Target Profile (Table 5) that is not adequately addressed in the Current Profile (Table 2) will be part of the new action plan. For example, in the Target Profile, it is desirable to have all sources of cyberthreat intelligence. Since the organization does not currently participate in any industry forum, ID.RA-2 is a part of the action plan. Similarly, subcategories that are in the Target Profile and are sufficiently addressed in the Current Profile are *not* a part of the action plan.

In subsequent iterations, this step will identify gaps between the current and target states and will provide an opportunity to add or update plans.

In light of the desired state, as described in the profile, the following action plans for protecting the cybersecurity of the satellite vehicle service are created.

To protect the satellite and its data from communications spoofing, interception, corruption, tampering, and denial of service:

1. In order to appropriately protect systems, the first task is to identify asset vulnerabilities and document those vulnerabilities as part of a cybersecurity program within the organization. This includes communicating with suppliers to understand their cybersecurity program. ID.RA-1, ID.SC-4.
2. Only allow authorized devices to communicate with the satellite, and employ the following requirements:
    a. Authenticate the claimed identity of any device attempting to communicate. CSF: PR.AC-1, PR.AC-6, PR.AC-7
    b. Drop all communication attempts for which the access authorization of the other device cannot be confirmed. CSF: PR.AC-3, PR.AC-4

c. Check the integrity of communications and drop any communications where integrity appears to have been violated. CSF: PR.DS-2

3. Only allow authorized devices to access sensitive data within the satellite's communications.

   a. Use encryption to protect the contents of communications. CSF: PR.DS-2, PR.DS-4

   b. Require that the recipient of encrypted communications be authenticated before they can decrypt the communications and access their contents. (See 1a above.)

4. Make the satellite's communications resilient to adverse conditions.

   a. Use communication protocols that ensure delivery. CSF: PR.PT-5

   b. Have a secondary or alternate communications channel available at all times, and automatically fail over to it when the primary communications channel is not functioning properly. CSF: PR.PT-5

   c. When communications are unavailable, store any unsent sensor data and send it after communications are restored. CSF: PR.PT-5

5. Build protections into the satellite to thwart DDoS-related connection attempts. CSF: PR.PT-4, PR.PT-5

6. Protect the vehicle if communications are compromised.

   a. Implementation of control PR. IP-9 response and recovery plans are in place in case the command-and-control link is attacked to ensure the safety of the vehicle, such as the ability to act in autonomous safe mode and to avoid collision in the case of a congested orbital slot.

7. Enhance the ability of the vehicle to ingest and share threat data and to react to that data. ID.RA-2

   b. Currently, threat information-sharing and decision-making happen in the ground segment. However, in the future, spacecraft may autonomously activate or deactivate an on-orbit function as a means to mitigate a potential attack. An additional enhancement of this would be automated threat-sharing that can be ingested by the vehicle.

To protect the satellite and its data from unauthorized access, use, corruption, tampering, and denial of service:

1. Use secure device design and development practices for the satellite hardware, firmware, operating system, and applications.

   a. Isolate executing processes from each other. See the SSDF publication.

   b. Validate all input, including commands and data (e.g., allow listings, input constraints). See the SSDF publication.

   c. Satellites typically have multiple redundant paths to account for failures in orbit. For example, the MIL-STD-1553 data bus has multiple redundant paths. The standard also calls for an "A" side and a "B" side for space vehicles and associated redundant hardware that will allow the satellite to operate if any component fails. The isolation of the data bus is logical, not physical, and space operators should consider isolation as part of their design, understanding the SWAP (i.e., size, weight, and power) impacts that this may produce.
   d. Build protections into the device for DoS attacks.
2. Prevent and deter attacks against the satellite.
   a. Use a hardware root of trust to perform a secure boot, which will be the basis for conducting system integrity checks and other health checks/self-tests. CSF: PR.DS-6, PR.DS-8
   b. Provide update, upgrade, and uninstall capabilities for firmware and software. (Also see items 1 and 2 above.) CSF: PR.IP-12
   c. Configure the satellite to avoid known security weaknesses. CSF: PR.IP-1, PR.IP-3
   d. Prevent unauthorized software from executing (e.g., anti-malware software, application allow listings software, code signing). CSF: DE.CM-4, DE.CM-7, PR.PT-3
3. Only allow authorized parties to access and alter sensor data stored on the satellite.
   a. Enforce the principle of least privilege. CSF: PR.AC-4, PR.DS-1
   b. Protect the integrity of all stored sensor data. CSF: PR.DS-1, PR.DS-6

To detect, respond to, and recover from attacks and incidents involving the satellite, its data, and its communications:

1. Log security-related events, and continuously review the logs. CSF: PR.PT-1, DE.AE-3, DE.CM-1
2. Investigate suspicious events. CSF: DE.DP-4, RS.AN-1, RS.AN-3, RS.CO-5
3. Prevent an incident from continuing or expanding (e.g., by failing safe). CSF: RS.MI-1
4. Recover from incidents by restoring data and software. RC.RP-1, RC.IM-2

To obtain the most current and accurate threat data to inform the residual risk analysis:

1. The organization joins a local Information Sharing and Analysis Center (ISAC) so that company representatives will have a venue for sharing and receiving prioritized information regarding known risks as the threat and technology landscapes evolve.
2. The organization defines a protocol to consult various authorities at the NASA, NOAA, FAA, Department of Homeland Security, and/or the Department of Defense to better understand potential threats to space-based network operations.

For Step 7 – Security leaders present the action plan, business case, and requests for appropriate resources to key company stakeholders and executives for approval. Processes to monitor and review the plan's implementation ensure that the activities sufficiently address cybersecurity risks to satellite operations, allow for future updates to the profiles, and maintain oversight over external service providers.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the Orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

4.3 Conclusion

NIST has provided this example to show how an organization might apply the steps of the Cybersecurity Framework to evaluate and address possible security risks. NIST recommends that organizations apply the steps that best apply to their threat models, business cases, and risk tolerance. As the industry expands, NIST will continue to support the community through research products and risk management guidance.

724 # References

[1] National Institute of Standards and Technology (2001) Security requirements for cryptographic modules (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS PUBS) 140-3, March 22, 2019. https://doi.org/10.6028/NIST.FIPS.140-3

[2] Joint Task Force Transformation Initiative Interagency Working Group (2013) Security and privacy controls for federal information systems and organizations (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[3] National Oceanic and Atmospheric Administration (2007) U.S. Leadership in Space Commerce: Strategic Plan for the Office of Space Commercialization (OSC) (U.S. Department of Commerce). Available at https://www.space.commerce.gov/wp-content/uploads/NOAA-2007-Space-Commercialization-Strategic-Plan-6-pages.pdf

[4] White House (2010) National Space Policy of the United States of America (White House, Washington, D.C.) Available at https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf

[5] 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

[6] National Institute of Standards and Technology (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

[7] Committee on National Security Systems (2012) National Information Assurance Policy for Space Systems Used to Support National Security Missions (Committee on National Security Systems, National Security Agency, Ft. Meade, MD), Committee on National Security Systems Publication (CNSSP) No. 12. Available at https://www.hsdl.org/?view&did=726945

[8] https://www.fcc.gov/general/international-bureau-satellite-division

[9] Licenses & Permits: Commercial Space Transportation (faa.gov)

[10] Pub. L. 111-314, Dec. 18, 2010, 124 Stat. 3409. Chapter 601, Land Remote Sensing Policy. Available at

https://www.nesdis.noaa.gov/CRSRA/files/National_and_Commercial_Space_Programs_Act_60101.pdf

[11] Federal Register, Vol. 71, No. 79, April 25, 2006. 15 CFR Part 960. Licensing of Private Land Remote-Sensing Space Systems. National Oceanic and Atmospheric Administration. Available at https://www.nesdis.noaa.gov/CRSRA/files/15%20CFR%20Part%20960%20Regs%202006.pdf

[12] https://www.nesdis.noaa.gov/CRSRA/licenseHome.html

[13] Hacking Satellites, Look Up Into the Sky, Infosec Institute September 18, 2013. Available at https://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky

[14] Hacking satellites, November 21, 2011. By Pierluigi Paganini SecurityAffairs.com. Available at http://securityaffairs.co/wordpress/236/cyber-crime/hacking-satellites.html

[15] How To Hack The Sky, Andy Greenberg, Forbes Staff, Feb 2, 2010. Available at https://www.forbes.com/2010/02/02/hackers-cybercrime-cryptography-technology-security-satellite.html

[16] Security Threats against Space Systems, CCSDS, December 2015. Available at https://public.ccsds.org/Pubs/350x1g2.pdf

Appendix A—Examples of Relevant Regulations

This appendix provides examples of regulations that may be relevant to some but not all commercial satellite operations. It is important for each organization to identify the potential regulation and regulatory agency that applies to their specific operations and business.

DoD/IC/NGA

From the *National Information Assurance Policy for Space Systems Used to Support National Security Missions* by the Committee on National Security Systems Publication (CNSSP) No. 12:

> Presidential Policy Directive (PPD-4), *National Space Policy of the United States of America*…reiterates that United States national security is critically dependent upon space capabilities and this dependence will grow. Space activities are also closely linked to the operation of the United States Government's (USG) critical infrastructures and have increasingly been leveraged to satisfy national security requirements. Therefore, increased assurance and resilience are needed for the mission-essential functions of national security space systems, including their supporting infrastructure, to help protect against disruption, degradation, and destruction, whether from environmental, mechanical, electronic, or hostile means.

> The primary objective of this policy [CNSSP-12] is to help ensure the success of national security missions that use space systems, by fully integrating information assurance into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems. Fully addressing information assurance is especially important for the space platform portion of space systems, since any vulnerability in them normally cannot be eliminated once launched.

Federal Communications Commission (FCC)

Regarding the International Bureau Satellite Division, Federal Communications Commission (FCC):

> The primary mission of the Satellite Division is to serve U.S. consumers by promoting a competitive and innovative domestic and global telecommunications marketplace. The Division strives to achieve this goal by:

1. Authorizing as many satellite systems as possible and as quickly as possible to facilitate deployment of satellite services;
2. Minimizing regulation and maximizing flexibility for satellite telecommunications providers to meet customer needs;
3. Fostering efficient use of the radio frequency spectrum and orbital resources. The Division also provides expertise about the commercial satellite industry in the domestic

spectrum management process and advocates U.S. satellite radiocommunication interests in international coordinations and negotiations.

Federal Aviation Administration (FAA)

Regarding the Office of Commercial Space Transportation:

> The Office of Commercial Space Transportation (AST) was established in 1984…as part of the Office of the Secretary of Transportation within the Department of Transportation (DOT). In November 1995, AST was transferred to the Federal Aviation Administration (FAA) as the FAA's only space-related line of business. AST was established to:

- Regulate the U.S. commercial space transportation industry, to ensure compliance with international obligations of the United States, and to protect the public health and safety, safety of property, and national security and foreign policy interests of the United States;
- Encourage, facilitate, and promote commercial space launches and reentries by the private sector;
- Recommend appropriate changes in Federal statutes, treaties, regulations, policies, plans, and procedures; and
- Facilitate the strengthening and expansion of the United States space transportation infrastructure.

National Oceanic and Atmospheric Administration (NOAA)

Regarding the Commercial Remote Sensing Regulatory Affairs (CRSRA) Licensing Program:

> This web site is intended to provide U.S. laws, regulations, policies, and guidance pertaining to the operation of commercial remote sensing satellite systems. Pursuant to the National and Commercial Space Programs Act (NCSPA or Act), 51 U.S.C. § 60101, et seq, responsibilities have been delegated from the Secretary of Commerce to the Assistant Administrator for NOAA Satellite and Information Services (NOAA/NESDIS) for the licensing of the operations of private space-based remote sensing systems.

> In accordance with the Act, the regulations 15 CFR Part 960 concerning the licensing of private remote sensing space systems have been promulgated.

Space Policy Directive 5 (non-regulatory)

> (SPD-5) Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems. Policy will foster practices across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations. SPD-5 states adoption by industry should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems.

Appendix B—Acronyms

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

AST	Office of Commercial Space Transportation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSP	Committee on National Security Systems Publication
CRSRA	Commercial Remote Sensing Regulatory Affairs
CSF	Cybersecurity Framework
CTO	Chief Technology Officer
DOT	Department of Transportation
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FOIA	Freedom of Information Act
IR	Internal Report
ITL	Information Technology Laboratory
LEO	Low Earth Orbit
NCSPA	National and Commercial Space Programs Act
NESDIS	National Environmental Satellite, Data, and Information Service
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
OSC	Office of Space Commercialization
PPD	Presidential Policy Directive

SDO	Standard Development Organization
SP	Special Publication
SSO	Standard Setting Organization
TT&C	Telemetry Tracking and Command
USG	United States Government

Appendix C—Glossary

beacon Initial signal by satellite conducted when first put into mission operation in order to establish communications with command and control and report initial operating status

bus The infrastructure of a space platform typically consisting of the basic physical structures, mechanisms, and subsystems for propulsion, power, thermal control, attitude determination and control, and TT&C (telemetry, tracking, and command) communications and processing

crosslinks Communication between satellites

current profile The ‘as is’ state of system cybersecurity

downlink Communication originating from the satellite to the ground

payload Mission-specific items of the overall satellite that are not part of the overall operations or “flying” of the satellite

profile A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories

risk The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring

satellite Bus and payload combined into one operational asset

space structures Term referring to “space debris” or “space junk” that is no longer in use for any business or mission need; any human-made assets in space

target profile The desired outcome or “to be” state of cybersecurity implementation

telemetry The science of measuring a quantity or quantities, transmitting the results to a distant station, and interpreting, indicating, and/or recording the quantities measured

threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; the potential for a threat-source to successfully exploit a particular information system vulnerability

umbilical cord During prelaunch, this cable connects the space vehicle to the launch pad to monitor the vehicle health and is disconnected or cut when the vehicle launches; enables the exchange of data with ground launch mission systems

uplink Communication originating from the ground to the satellite

vehicle Space operational items that include the launching items used to place the satellite, bus, and/or payload into orbit

vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source