**NISTIR XXX**

**Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Command and Control of Satellite Bus and Payloads**

Suzanne Lightman

Theresa Suloway

Doug Northip

Joseph Brule

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

**NISTIR XXXX**

**Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Command and Control of Satellite Bus and Payloads**

|  |
| --- |
|   |
|  Suzanne Lightman  | Theresa Suloway  |
|  *Computer Security Division*  *Information Technology Laboratory*   | Doug Northrip Joseph Brule |
|  | *The MITRE Corporation*  |
|  | *McLean, VA*  |
|  |  |
|  |  |
|  |  |
|  |  |
|   |  |
|  |  |

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



U.S. Department of Commerce

*Wynn Coggins, Acting 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 XXXX

XXX pages (*month* 2021) This publication is available free of charge from:

https://doi.org/10.6028/NIST.IR.XXXX

This document was published initially as a draft on Month, Day Year, with a 30-day public comment period.

 Revisions and updates were incorporated into the final version.

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.

**Comments on this publication may be submitted to:**

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000 Email: mailto: pnt-eo@list.nist.gov

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

The critical infrastructure, to include space operations are essential to the national and economic security of the United States (US). 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 COMSAT bandwidth, purchase of commercial imagery, the hosting of government payloads on commercial satellites etc. The US government recognizes and supports space resiliency as illustrated by numerous space policies, the cyber security strategy and executive orders. The space cyber-ecosystem is an inherently risky, high cost and often inaccessible environment that consists 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

critical infrastructure; Cybersecurity Framework; risk management; space operations.

### Acknowledgments

The authors wish to thank all individuals, organizations, and enterprises that contributed to the creation of this document. This includes …

### 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 NISTIR XXXX [publication details.](https://csrc.nist.gov/publications/detail/nistir/8323/final)

### Patent Disclosure Notice

*NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.*

*As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.*

*No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.*

|  |
| --- |
| **Executive Summary**  |

Will be written after the final draft.

### Table of Contents

To be supplied

### List of Appendices

Informative references

Acronyms

Glossary

Additional resources

### List of Figures

To be supplied

|  |  |
| --- | --- |
| **1**  | **Introduction**  |

This document focuses on the ground segment. 8270 (draft) focuses on the space segment. 8323 was written for PNT users. The user segment will most likely require a suite of profiles for IMINT, sensors, COMSATS, telephony etc.

Space is an increasingly important element of the critical infrastructure. The impact of a loss or degradation of space services would be severe to the security and economic wellbeing of the United States. The USG recognizes that government owned space operations can be augmented with the commercial space industry through activities such as the leasing of commercial COMSAT bandwidth, commercial space-based telecommunications, the purchase of commercial imagery, the use of commercial satellite buses to host USG payloads, and other capabilities. This report provides a general introduction to Cybersecurity Framework as applied to the commercial space industry’s ground segment. The intent is to introduce basic concepts, generate discussions, refine understandings, and provide references for additional information on pertinent cybersecurity risk management concepts. The Cybersecurity Framework provides a means for stakeholders to assess their security posture in terms of identification, protection, detection, response, and recovery operations and derive a plan to elevate risk posture. This document is by no means comprehensive in terms of addressing all cybersecurity risks to commercial space infrastructure, nor does it provide implementation guidance. ***The scope of this document is the operational phase of the commercial space ground segment.*** Stakeholders are referred to other documents for guidance on assuring security policy integrity for the space vehicle initiatives and user 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 establishing defined and repeatable risk management approaches to elevate actual state to a defined desired state. The Profile provides methodology to classify systems, processes, and components of satellite command, control, and payload systems to determine the risk posture and address the residual risk in the management and control of the space segement. 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 station and supporting infrastructure;
* Protect the systems that the ground segment relies on through policy, role certification, training, resiliency, and access control;
* Detect a loss of the ground segments’ confidentiality, integrity, or availability;
* Respond to breaches of confidentiality, a manipulation or loss of satellite bus or payload 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 Profile’s scope includes any system, network, or capability that interacts with a satellite bus or payload for purposes of querying, commanding, or receiving telemetry. The Profile’s scope does not include the space vehicle itself or the user segment of the space system. This Profile will support the stakeholder’s ability to;

* Make risk-informed decisions about the cybersecurity of the space segment’s bus and payload;
* Select risk-based approaches that minimize the potential effects of the disruption or manipulation satellite bus and payload commanding; and
* Consider planning and action regarding the secure management and recovery of the space segment.



**Not in Scope**

**Not in Scope**

**Not in Scope**

**Figure 1 – AEROSPACE CORP has a better graphic. In process of getting permission to use.**

1.3 Audience

The intended audience includes public and private organizations that own, operate or manage space systems such as:

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

This publication is for use by both public and private organizations that own, operate or manage space systems and/or are seeking to elevate current security postures.

The Profile is suitable for a range of stakeholders with varying degrees of risk management experience including organizations.:

* That have already adopted the NIST Cybersecurity Framework (CSF) to help identify, assess, and manage cybersecurity risks [NIST CSF];
* Are familiar with the CSF and want to improve their risk posture;
* Are unfamiliar with the CSF but need to implement risk management frameworks.

|  |  |
| --- | --- |
| **2**  | **Intended Use**  |

EDITORIAL NOTE: The portions in yellow will not be included in the document. Intended to stimulate reviewers comments. Sector level profiles provide a starting point and an organization will tailor and/or augment a profile.

The Profile is a flexible tool that an organization can use as a part of its risk management effort. This profile is intended to augment, not 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:

* What ground segment processes and assets are dependent on other assets (i.e., what are the externalities and secondary effects)?
* What is the level of interconnectivity of the ground segment with other processes?
* What processes and assets are vulnerable?
* What are the integrity and availability thresholds to avoid mission impact?
* What safeguards are currently in place?
* What is the impact to the organization should a process or asset be lost or degraded?
* What techniques can be used to detect events of concern?
* What techniques can be used to respond to events of concern?
* What techniques can be used to recover to pre-event capabilities?
* What techniques are leveraged to measure effectiveness of implemented policies and methodologies to iteratively revise incumbent security policies

|  |  |
| --- | --- |
| **3**  | **Overview**  |

#### 3.1 Risk Management Overview

EDITORIAL NOTE: The portions in yellow will not be included in the document. Intended to stimulate reviewers comments. Profiles are a *part* of risk management; this section is intended to orient the reader.

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 the probability and likelihood that an event will occur as well as its potential impacts. 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 800-39. 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:[[1]](#footnote-2)

1. The Framework Core provides a catalog of desired cybersecurity activities and outcomes[[2]](#footnote-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.
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 the 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 act regarding a detected cybersecurity incident. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event.
5. Recover – Develop and implement the appropriate activities to maintain plans for 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 improvements.

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” or “Protective Technology.”

EDITORIAL NOTE: The portions in yellow will not be included in the document. Intended to stimulate reviewers comments. This graphic is from 8270, a different graphic was presented in 8323.



The CSF is outcome based and focuses on the cybersecurity functions rather than components. A CSF profile is not intended to provide specific implementation guidance; however, a profile will supply informative references to existing standards, guidelines, and practices that provide practical guidance to help an organization achieve the desired outcome of each Subcategory. An example of two Subcategories and applicable References within the Asset Management Category are shown in Figure 2.

**Figure 2 - Cybersecurity Framework Subcategory Example**



|  |  |
| --- | --- |
| **4**  | **Baseline Profile**  |

EDITORIAL NOTE: The portions in yellow will not be included in the document. Intended to stimulate reviewers comments. Request industry’s insight regarding ‘typical’ architectures and ‘typical’ concept of operations. The assumptions guide which subcategories the reader needs to focus on vs which subcategories the reader only needs to be aware of.

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 references provide additional guidance.

Organizations should select, tailor, and augment the functions, categories and subcategories presented in Sections 4.1 through 4.5 in accordance with their risk tolerance, security architecture, and controls. 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 the subcategories (to include those considered not applicable) in the context of their organization***.

This baseline profile focuses on two high level ground segment missions.

* A Satellite Operations Center (SOC) issues commands to a space vehicle’s bus and receives telemetry from a space vehicle’s bus.
* A SOC may issue commands to and receives 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 SOC.

It is assumed that the SOC has the following architectural characteristics and operational procedures:

* Remote components to the SOC (such as antenna fields auxiliary stations etc.) are connected to the SOC via encrypted permanent virtual circuits or virtual private networks. EDITORIAL NOTE: The portions in yellow will not be included in the document. Intended to stimulate reviewers comments. Do commercial SOCs use PVC’s or VPNs to connect to the antenna fields?
* Access to the SOCs are strictly limited and critical assets (such as workstations and components that command the space segment) are air gapped.[[3]](#footnote-4) Are the workstations that connect to the space segment single purpose stand alone or are they connected to the satellite AND the internet?
* Connections between SOC facilities and antenna fields are wired or encrypted RF.
* Virtualized devices are hosted on private or hybrid clouds. Intended to stimulate reviewers comments. Does industry use public clouds?
* Remote access to the SOC from devices that are not controlled and managed by the organization is prohibited for normal operations. Does industry allow remote logins or teleworkers to command a satellite?
* Physical access to the SOC is controlled by measures such as guards, gates, badges, PINs etc.
* Actions that can potentially damage or lose control of the space segment require multiple commands.
* Personal computing and communication devices such as laptops, cell phones are not permitted within the facilities that house workstations and equipment that directly interface with the space segment. Is this an accurate assumption in the commercial world?

Scenarios such that a satellite is hosting one or more third party payloads:

* Commands are generated by the payload SOC, transmitted by the bus SOC routed through the bus command module to the payload.
* All third party bus and payload commands are encrypted and cryptographically isolated from each other. When commercial companies host payloads, is it an industry best practice to cryptographically isolate the bus and payload(s)?
* Payload communications (to include telemetry, state of health, responses etc.) are downlinked to the payload SOC rather than being routed through the bus SOC.
* Telemetry and state of health are logically separated, but not necessarily cryptographically isolated.
* A payload SOC does not directly interact with the space vehicle’s bus. Pointing, attitude or any bus related request is issued to the bus SOC.

The functions, categories, and subcategories as they pertain to SOCs are TO BE SUPPLIED

Appendices TO BE SUPPLIED

1. Elements of the Cybersecurity Framework—including Core, Implementation Tiers, Profile, Function, Category, and Subcategory—are normally capitalized and will be capitalized throughout this document. [↑](#footnote-ref-2)
2. The word “outcomes” is used because the Cybersecurity Framework (CSF) 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 how they will achieve it. The References described on page 8 help organizations with the “how.” [↑](#footnote-ref-3)
3. Reference: page 5 Best Practices for Protection of Commercial Satellite Communications Infrastructure AIAA 2006-5386 [↑](#footnote-ref-4)