Withdrawn White Paper

Warning Notice

The attached white paper has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date June 6, 2023

Original Release Date November 3, 2022

Superseding Document

Status Initial Public Draft

Series/Number NIST Interagency Report (IR) 8441

Title Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)

Publication Date June 2023

DOI https://doi.org/10.6028/NIST.IR.8441.ipd

CSRC URL https://csrc.nist.gov/pubs/ir/8441/ipd

Additional Information

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

NIST Cybersecurity White Paper
NIST CSWP 27

Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)

Final Annotated Outline

James McCarthy
National Cybersecurity Center of Excellence
Applied Cybersecurity Division
Information Technology Laboratory

Dan Mamula
Joseph Brule
Karri Meldorf
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.27

November 2022

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

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on 2022-10-24

How to Cite this NIST Technical Series Publication:

McCarthy J, Mamula D, Brule J, Meldorf K (2022) Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN): Final Annotated Outline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 27. https://doi.org/10.6028/NIST.CSWP.27

Author ORCID iDs

James McCarthy: 0000-0002-5559-733X
Karri Meldorf: 0000-0003-3617-3846

Contact Information

hsn_nccoe@nist.gov

National Institute of Standards and Technology
Attn: National Cybersecurity Center of Excellence
9700 Great Seneca Highway (Mail Stop NIST) Rockville, MD 20850

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

Abstract

The objective of this Cybersecurity Profile is to identify an approach to assess the cybersecurity posture of Hybrid Satellite Networks (HSN) that provide services such as satellite-based systems for communications, position, navigation, and timing (PNT), remote sensing, weather monitoring, and imaging. The HSN systems may interact with other government systems and the Critical Infrastructure as defined by the Department of Homeland Security to mutually increase their resilience. This Profile will consider the cybersecurity of all the interacting systems that form the HSN rather than the traditional approach of a single organization acquiring the entire satellite system that includes the satellite bus, payloads, and ground system.

NIST is developing a consistent approach to assess the cybersecurity posture of a space system to facilitate the better understanding of the attack surface, incorporate security, and achieve greater resilience for space systems that may be leveraged by critical infrastructure owners and operators, the Department of Defense, or other government missions.

Keywords

cybersecurity; data transport; ground system; hosted payload; space; spacecraft.

Additional Information

For additional information on NIST's Cybersecurity programs, projects, and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

Table of Contents

1. HSN Cybersecurity Framework Profile – Introduction 1
1.1. Background 1
1.2. Purpose and Objectives 1
1.3. Scope 2
1.4. Audience 2
2. How to Use the HSN Cybersecurity Framework Profile 3
3. HSN Cybersecurity Profile – Overview 3
3.1. Risk Management Overview 4
3.2. Capabilities Overview 4
3.2.1. Policies and Procedures 5
3.2.2. Security Technical Capabilities Overview 5
3.3. The HSN Cybersecurity Profile 5
Appendix A. Acronyms 5
Appendix B. Selected Bibliography 6

1. Hybrid Satellite Networks Cybersecurity Framework Profile – Introduction

A significant level of sensing, communications, and PNT capabilities is being provided by the space sector, and there is a growing trend toward multi-national/ multi-organizational consortia providing these services. Hybrid Satellite Networks (HSN) present opportunities for organizations to leverage existing space-based capabilities through means such as hosted payloads; however, there is a need to ensure that these systems are secure, and that the integration of the components is done in a manner that is acceptable to the participating organizations.

The HSN cybersecurity profile (hereafter, the Profile) is intended to provide a means to assess and communicate an organization's cybersecurity posture in a consistent and standardized manner. The Profile applies to 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 cybersecurity postures; and
- are unfamiliar with the CSF but need to implement HSN services in a risk informed manner through the use of a cybersecurity risk management frameworks.

1.1. Background

The space sector is transitioning towards an aggregation of independently owned and operated segments that create a space system, rather than the traditional approach where a single entity acquires, operates and controls the space, ground and user segments. To provide guidance to space stakeholders, NIST, in a partnership with industry, is developing this profile. Throughout the Profile development process, NIST will engage the public and private sectors on multiple occasions to include a request for information, participation in workshops, and comment and review of the draft Profile. The Profile development process is iterative and, in the end state, promotes the risk informed use of Hybrid Satellite Networks.

1.2. Purpose and Objectives

The purpose of the Profile is to provide practical guidance for organizations and stakeholders engaged in the design, acquisition, and operation of satellite buses or payloads that involve HSN.

A completed Profile for commercial satellite companies operating in a hybrid environment that includes government and commercial entities will provide for future cybersecurity resilience. The Profile is suitable for applications that involve multiple stakeholders contributing to communications architecture and for other use cases such as hosted payloads. Use of the HSN Profile will help organizations;

- Identify systems, assets, data and threats that pertain to HSN;
- Protect HSN services by adhering to basic principles of resiliency;
- Detect cybersecurity-related disturbances or corruption of HSN services and data;

- Respond to HSN service or data anomalies in a timely, effective, and resilient manner; and
- Recover the HSN to proper working order at the conclusion of a cybersecurity incident.

1.3. Scope

The Profile will document an example architecture for data transport through hybrid satellite networks. The architecture will describe the salient cybersecurity functions that are part of the HSN to highlight cybersecurity dependencies.

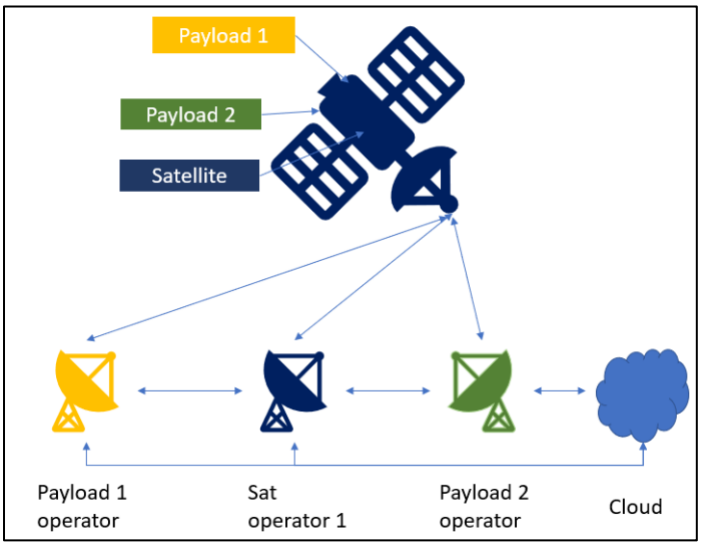

Fig. 1. Example HSN Architecture

The Profile will focus on the complex variety of interfaces, data flows, and space stakeholders involved in modern satellite communications networks. The CSF profile is intended to:

- Facilitate integration of HSN components thorough consideration of cybersecurity functions, categories, and subcategories.
- Assess cybersecurity posture in a consistent manner.
- Provide a comprehensive framework to facilitate risk management decisions.
- Facilitate consistent assessment of cyber-risk.
- Communicate cybersecurity posture and priorities in a consistent manner.

The Profile provides a subset of CSF subcategories that is directly applicable to the HSN and mitigation strategies that could be implemented. The Profile allows each organization the flexibility to implement selected mitigation strategies based on their risk posture or accepted risk management strategy.

1.4. Audience

This document is intended to be used by those involved in overseeing, developing, implementing, and managing the HSN cybersecurity of systems such as:

- Public and private organizations that provide HSN services;
- Managers responsible for the use of HSN services;
- Risk managers, cybersecurity professionals, and others with a role in cybersecurity risk management for systems that use HSN services;
- Procurement officials responsible for the acquisition of HSN services;
- Mission and business process owners responsible for achieving operational outcomes dependent on HSN services;
- Researchers and analysts who study the unique cybersecurity needs of HSN services; and

Cybersecurity Architects who integrate Cybersecurity into the Product Designs for Space Vehicle Segments and Ground Segments.

2. How to Use the HSN Cybersecurity Framework Profile

The Profile will help organizations develop cybersecurity HSN profiles that are appropriate for their respective organization and goals. The Profile is intended to help users of HSN prioritize necessary cybersecurity activities based on their objectives. The Profile may be a tool to help organizations identify areas where standards, practices, and other guidance could help manage the risk of cybersecurity threats to systems that use or provide components to HSN.

The Profile is intended to assist an organization's risk management effort. The Profile does not prescribe regulations or mandatory practices, nor does it carry any statutory authority.

The development of a Profile by an organization is a multi-step process, including a risk assessment in which organizations should consider the following:

- What data, processes, and assets do HSN's require?
- What processes and assets are dependent recipients of HSN data (i.e., identify secondary effects)?
- What is the impact to the organization should a process or asset be lost or degraded?
- What processes and assets are vulnerable?
- What safeguards are available?
- What techniques can be used to identify threats of concern?
- What techniques can be used to respond to threats of concern?
- What techniques can be used to return an HSN to proper working order?

3. HSN Cybersecurity Profile – Overview

This section contains an overview of envisioned Profile content and a short description of the kinds of HSN services that are covered by the Profile. The Profile provides information on risk management, cybersecurity capabilities, and applies to the NIST Cybersecurity Framework to

assist with specific implementation of PNT cybersecurity. The Profile will include informative references (including existing standards, guidelines, and practices) and a glossary of terms.

3.1. Risk Management Overview

Risk management is the ongoing process of identifying, assessing, and responding to risk as related to an organization's mission objectives. To manage risk, organizations should understand the likelihood that an event will occur as well as its potential impacts. With this information, the government can determine the acceptable level of risk to the HSN data and services they use to achieve their mission objectives.

As an organization analyzes its mission objectives as they relate to reliance on or use of HSN data, there are a series of guiding questions that inform the process. They include:

- How can the supply chain cybersecurity threats impact the mission of the system?
- What are the threats to achieving mission objectives?
- What damages can result when those mission objectives are disrupted?
- What are the most important assets for a given mission objective?
- Where does physical infrastructure affect cybersecurity infrastructure and vice versa?

An organization should also be aware of statutory and policy requirements that may have a security or safety dimension. These can be affected by cybersecurity risk or create risks downstream.

The Profile supports and is informed by cybersecurity risk management processes. Using the Profile, organizations can make more informed decisions to select and prioritize cybersecurity activities and expenditures that help identify systems dependent on HSN, identify appropriate HSN sources, detect disturbances and manipulation of HSN services, manage the risk to these systems, and ensure resiliency through diversity. For critical infrastructures, HSN sources and distribution networks should be architected with multiple, independent sources; communication paths; and communication mediums. The Profile provides a starting point from which organizations can customize—based on business need and risk assessment—to develop the most appropriate processes to manage cybersecurity risk to their HSN services and data essential for the correct behavior of critical infrastructure applications.

Organizations can use the HSN Profile in conjunction with existing cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2018, ISO/International Electrotechnical Commission (IEC) 27005:2018, and NIST Special Publication 800-39. A list of helpful resources will be listed in an Annex of the Cybersecurity HSN Profile.

3.2. Capabilities Overview

This section describes some of the capabilities and controls that impact the organization's ability to manage residual risk (in the context of HSN degradation or outage).

3.2.1. Policies and Procedures

Cybersecurity policies and procedures will vary in accordance with each organization's tolerance of a HSN loss or degradation. Though it does not add value to burden an organization with excessive requirements, there should be a level of consistency within a sector to enable collaborative efforts, such as the sharing of cybersecurity events that impact or otherwise involve HSN. Consistency also facilitates the acceptance or rejection of inherited risk and compatible tools; techniques and processes enable coordinated responses.

HSN policies and procedures should be reflected in an organization's continuity of operations plan (COOP).

3.2.2. Security Technical Capabilities Overview

HSN resiliency requires organizational planning that includes an adequate understanding of the technical capabilities needed to ensure appropriate levels of HSN data confidentiality, availability, and integrity.

When considering the technical capabilities as they pertain to HSN resilience, users must consider certain technical challenges that a HSN service may encounter such as propagation delay for geosync, interference events, radiation, and other space environment related concerns.

It is beneficial to consider that the analysis of potential integration of multiple and independent technologies can facilitate the detection of anomalies, and ultimately contribute to a more resilient system in the event of a disruption.

3.3. The HSN Cybersecurity Profile

This section will contain the HSN Cybersecurity Profile, which applies the functions, categories, and sub-categories of the CSF, informative references to the HSN cyber ecosystem. This section contains information on how users of the profile can mitigate risks that they have deemed necessary to address based on their assessment of the HSN services they are using. This is not an exhaustive list, and the actual selection of controls (if any) must be based on a cost-benefit analysis that is consistent with the risk. Examples of space related CSF profiles can be found in the references section below.

Appendix A. Acronyms

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

CSF
Cybersecurity Framework

DoD
Department of Defense

HSN
Hybrid Satellite Networks

PNT
Positioning, Navigation, and Timing

RF
Radio Frequency

SSC
Space Systems Command

Appendix B. Selected Bibliography

The following NIST documents are provided as references for the audience to gain a clearer understanding of what the final HSN Cybersecurity profile will appear as. Included below are the NIST Cybersecurity Framework (CSF) along with two space technology sector profiles that were derived from the CSF.

- Bartock M, Lightman S, Li-Baboud Y-S, McCarthy J, Reczek K, Brule J, Northrip D, Scholz A, Suloway T (2022) **Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services**. National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8323r1 ipd, Initial Public Draft. https://doi.org/10.6028/NIST.IR.8323r1.ipd
- Lightman S, Suloway T, Brule J (2022) **Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control**. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8401 ipd, Initial Public Draft. https://doi.org/10.6028/NIST.IR.8401.ipd
- National Institute of Standards and Technology (2018) **Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.** (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6