Cybersecurity Profile for the Hybrid Satellite Networks (HSN) Cybersecurity

DRAFT Annotated Outline

Initial Public Draft

James McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Dan Mamula
MITRE Corporation
Gaithersburg, MD

Joseph Brule
MITRE Corporation
Gaithersburg, MD

Karri Meldorf
MITRE Corporation
Gaithersburg, MD

July 12, 2022

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

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

Abstract

The objective of this Cybersecurity Profile is to identify an approach to assess the cybersecurity posture of Hybrid Satellite Networks (HSN) systems 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 provide increased resiliency. This Profile will consider the cybersecurity of all the interacting systems that form the HSN rather than the traditional approach of the government acquiring the entire satellite system that includes the satellite bus, payloads, and ground system.

NIST is developing a consistent approach to better understand the attack surface, incorporate security, and achieve greater resilience for space systems that may be leveraged by critical infrastructure owners and operators, the DoD, or other government missions.

Keywords

cybersecurity; ground system; hosted payload; space; spacecraft

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

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.

Public comment period: July 12, 2022 – August 9, 2022

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

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

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

58 **Table of Contents**

70

1 HSN Cybersecurity Profile – Introduction

A significant level of sensing, communications, and PNT capabilities are 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 the integration of the components are 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];
- Organizations that are familiar with the CSF and want to improve their cybersecurity postures; and
- Organizations that 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 Systems Command (SSC) is charged with acquisition of space-based programs for the U.S. Space Force. This includes acquisition of satellite-based systems for communications, PNT; remote sensing, weather monitoring, and imagery. SSC's programs are increasing the use of commercial space through means such as hosting payloads on commercial satellites and services to meet mission objectives.

In an effort to partner with industry and leverage cybersecurity lessons learned, SSC in collaboration with NIST and the public and private sectors will create the HSN 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.

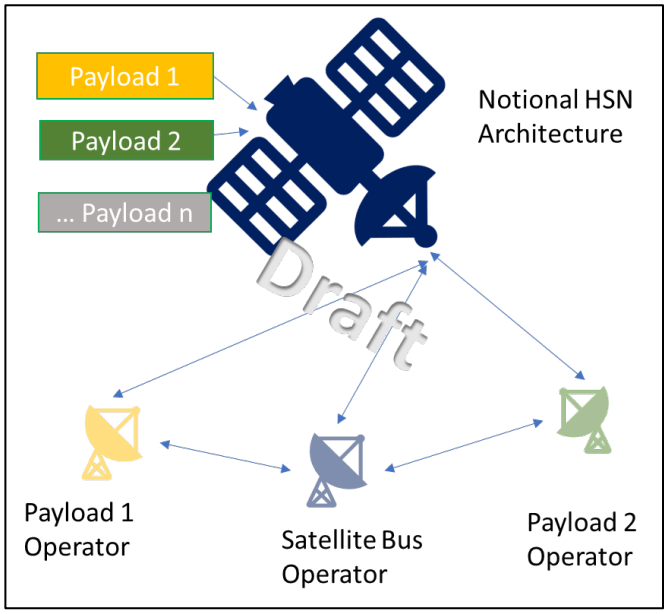
A completed Profile for commercial satellite companies operating in a hybrid environment that includes government and commercial entities will provide for future cybersecurity resilience. The Profile is suitable for applications that involve multiple stakeholders contributing to communications architecture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

Profile will help organizations ;

- Identify systems that provide HSN services;
- Identify data that originated from HSN sources;
- Protect HSN services by adhering to basic principles of resiliency;
- Detect cybersecurity-related disturbances or corruption of HSN services and data;
- Address cybersecurity risk in their management and use of HSN services and data;
- Identify common threats to systems that leverage 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 and may include operational views (OVs) to highlight cybersecurity dependencies.



The Profile will focus on the complex variety of interfaces, data flows, and institutions/actors 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 and communicate cybersecurity posture in a consistent manner
- Povide a comprehensive framework to facilitate risk management decisions.
- Facilitate consistent analysis of cyber-risk
- Communicate cybersecurity posture and priorities in a consistent manner

The Profile identifies a subset of CSF subcategories that are directly applicable to HSN while giving organizations the flexibility to mitigate cyber risk for their unique environment.

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; and
- Researchers and analysts who study the unique cybersecurity needs of HSN services.

2 How to Use the HSN Cybersecurity Profile

The Profile will help organizations develop cybersecurity HSN profiles that are appropriate for their respective organization and goals. The Profile will help organizations determine cybersecurity risks based on their assessments of the potential impacts of the manipulation, disruption, or loss of HSN services to business and operational objectives. 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 may wish to 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 mapping 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:

- 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 full list of helpful resources will be listed in an Annex of the Cybersecurity HSN Profile.

3.2 Capabilities Overview

The 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 maps the functions, categories, and sub-categories of the CSF with informative references. 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.

3.3.1 Detection of Disruptions to HSN Services

System verification and validation policy and procedures. Organizations should identify steady state and transient test cases, test plans, and test schedules as an end user, applicable to the industry supply chain, to serve as a basis for verifying and validating HSN data users in order to manage assessed risks associated with HSN disruptions.

3.3.2 Resilience of HSN Services

The ability to provide useable HSN data despite a compromise can be accomplished with technologies such as HSN component diversity and segmentation.

246 ## References

[NIST CSF] Framework for Improving Critical Infrastructure Cybersecurity. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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	**Position, Navigation, and Timing**
RF	**Radio Frequency**
SSC	**Space Systems Command**