Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)

Initial Public Draft

James McCarthy
Dan Mamula
Joseph Brule
Karri Meldorf
Rory Jennings
John Wiltberger
Chris Thorpe
John Dombrowski
O'Ryan Lattin

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

Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)

Initial Public Draft

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

Dan Mamula
Joseph Brule
Karri Meldorf
Rory Jennings
John Wiltberger
Chris Thorpe
John Dombrowski
O'Ryan Lattin
The MITRE Corporation

June 2023

38 Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in
39 this paper in order to specify the experimental procedure adequately. Such identification does not imply
40 recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or
41 equipment identified are necessarily the best available for the purpose.

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

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

58 **Author ORCID iDs**
59 James McCarthy: 0000-0002-5559-733X
60 Dan Mamula: 0000-0003-4247-1735
61 Karri Meldorf: 0000-0003-3617-3846
62 Joseph Brule: 0000-0002-7987-6050
63 O'Ryan Laffin: 0000-0003-4255-280X
64 Chris Thorpe: 0000-0001-6183-2300
65 Rory Jennings: 0000-0001-5860-5094
66 John Dombrowski: 0000-0002-9408-1838
67 John Wiltberger: 0000-0002-6412-8105

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

Abstract

The space sector is transitioning away from traditional vertically-integrated entities and towards Hybrid Satellite Networks (HSN) which is an aggregation of independently owned and operated terminals, antennas, satellites, payloads, or other components that comprise a satellite system. The elements of an HSN may have varying levels of assurance.

HSNs may interact with government systems and critical infrastructure (as defined by the Department of Homeland Security). A framework is required to assess the security posture of the individual components while still enabling the HSN to provide its function. This report applies the NIST Cybersecurity Framework to HSNs with an emphasis on the interfaces between the participants of the HSN.

In collaboration with subject matter experts including satellite builders, consultants, acquisition authorities, operators (commercial and government), academia, and other interested parties, the National Institute of Standards and Technology (NIST) has developed the HSN Cybersecurity Framework CSF Profile (HSN Profile) to guide space stakeholders. The resulting profile provides a starting point for stakeholders who are assessing the cybersecurity posture of their HSN.

Keywords

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.

104 **Call for Patent Claims**

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

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

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

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

118   i.   under reasonable terms and conditions that are demonstrably free of any unfair
119   discrimination; or

120   ii. without compensation and under reasonable terms and conditions that are
121   demonstrably free of any unfair discrimination.

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

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

129 Such statements should be addressed to: hsn_nccoe@nist.gov.

130 **Table of Contents**

List of Tables

List of Figures

Acknowledgments

1. Introduction

The space sector is transitioning away from traditional vertically integrated entities and towards an aggregation of independently owned and operated segments.

A Hybrid Satellite Network (HSN) utilizes multiple terrestrial and space components to provide extended global services across diverse missions and connecting points. The HSN architecture may consist of independently owned terminals, antennas, satellites, payloads, or other components that communicate across disparate networks. HSN system services may include satellite-based communications, position, navigation, and timing (PNT), remote sensing, weather monitoring, and imaging. These systems may interact with government systems and critical infrastructure (as defined by the Department of Homeland Security). These systems may have varying levels of trust among different components, requiring frameworks for establishing confidentiality and integrity of individual components while still enabling availability of required shared services.

HSN architectures provide secure, scalable, responsive, cyber resilient and information-centric opportunities. The flexibility of HSNs enables rapid and secure integration of new technologies.

HSNs present opportunities for organizations to leverage existing space-based capabilities and platforms through means such as hosted payloads, ground infrastructure as a service, virtualized satellite operation centers, etc. There is a need to verify that these systems are secure, and that the integration of components is done in a manner acceptable to the participating organizations. In collaboration with subject matter experts including satellite builders, consultants, acquisition authorities, operators (commercial and government), academia, and other interested parties, the National Institute of Standards and Technology (NIST) has developed the HSN Cybersecurity Framework CSF Profile (HSN Profile) to guide space stakeholders.

1.1. Purpose and Objectives

The HSN profile provides practical guidance for organizations and stakeholders engaged in the design, acquisition, and operation of satellite buses or payloads in a manner consistent with the organization's risk tolerance.

The HSN profile is suitable for applications that involve multiple stakeholders contributing to imagery, sensing, broadcast, communications, or other space-based architectures. Use of the HSN profile will help organizations:

- Identify systems, assets, data, and risks that pertain to HSN.

- Protect HSN services by performing self-assessments and adhering to cybersecurity principles.

- 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.

- Recover the HSN to proper working order after a cybersecurity incident.

246   **1.2.   Scope**

247   The HSN profile will describe the salient cybersecurity functions that are part of the HSN and
248   may include examples to highlight cybersecurity dependencies. Different business objectives or
249   mission requirements will require unique relationships between components of the HSN. These
250   requirements will dictate how data exchanges between system components, ranging from routing
251   data to rendering and analyzing data procured between components.
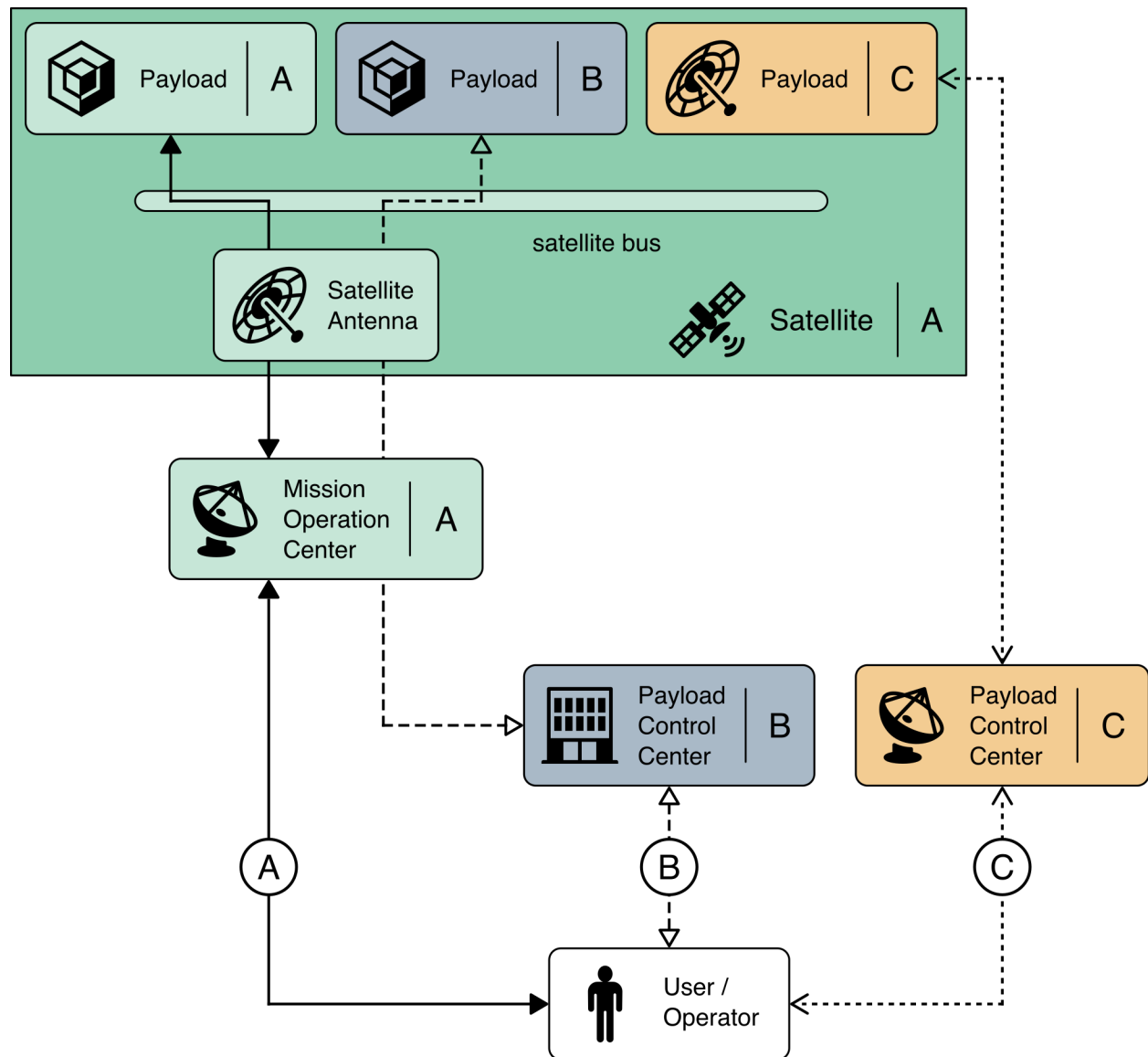
252   **Fig. 1.** Example of a simple HSN Architecture.

253   **NOTE:** The solid line indicates a normal path while the dashed lines depict communication
254   paths that may be present in an HSN.

255   A simple satellite architecture is depicted in Fig. 1. Path A shows a typical satellite
256   communications path (non-HSN). In a hybrid environment, the satellite bus and payloads B and
257   C are independently owned and operated where the host system provides different level of
258   services. Fig. 1 shows payload C relies on the host satellite for power and satellite operations
259   while payload B relies on the host for communications in addition to power and satellite
260   operations.
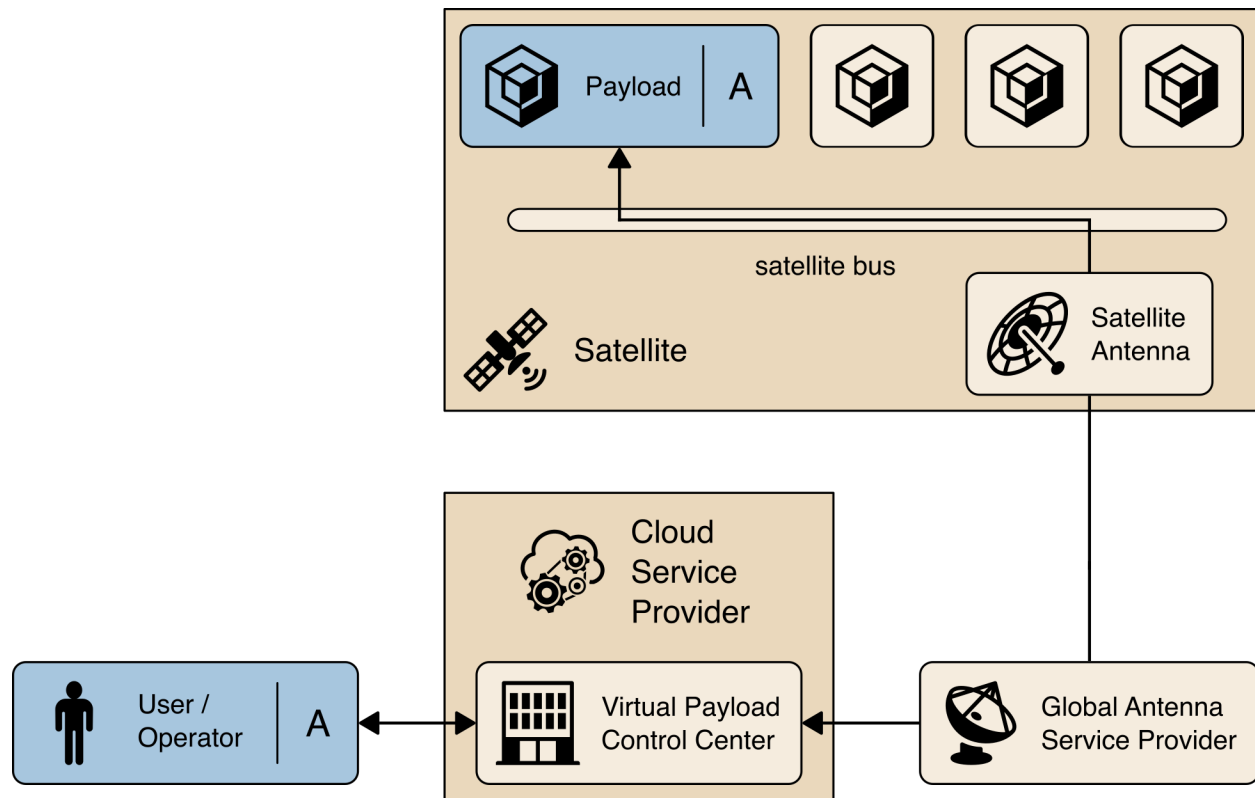
261   **Fig. 2.** Example of an HSN with virtualized components.

262   The elements of an HSN may be independently owned, hosted, or virtualized by multiple
263   organizations. While referring to Fig. 2, note that the operator may own the intellectual property
264   that defines the virtualized payload control center (PCC) which is hosted on a third-party cloud
265   service provider (CSP). The virtual PCC interfaces with a physical antenna field independent of
266   the CSP, the operator, and the satellite antenna, yet the operator in organization A can seamlessly
267   command, control and communicate with payload A.
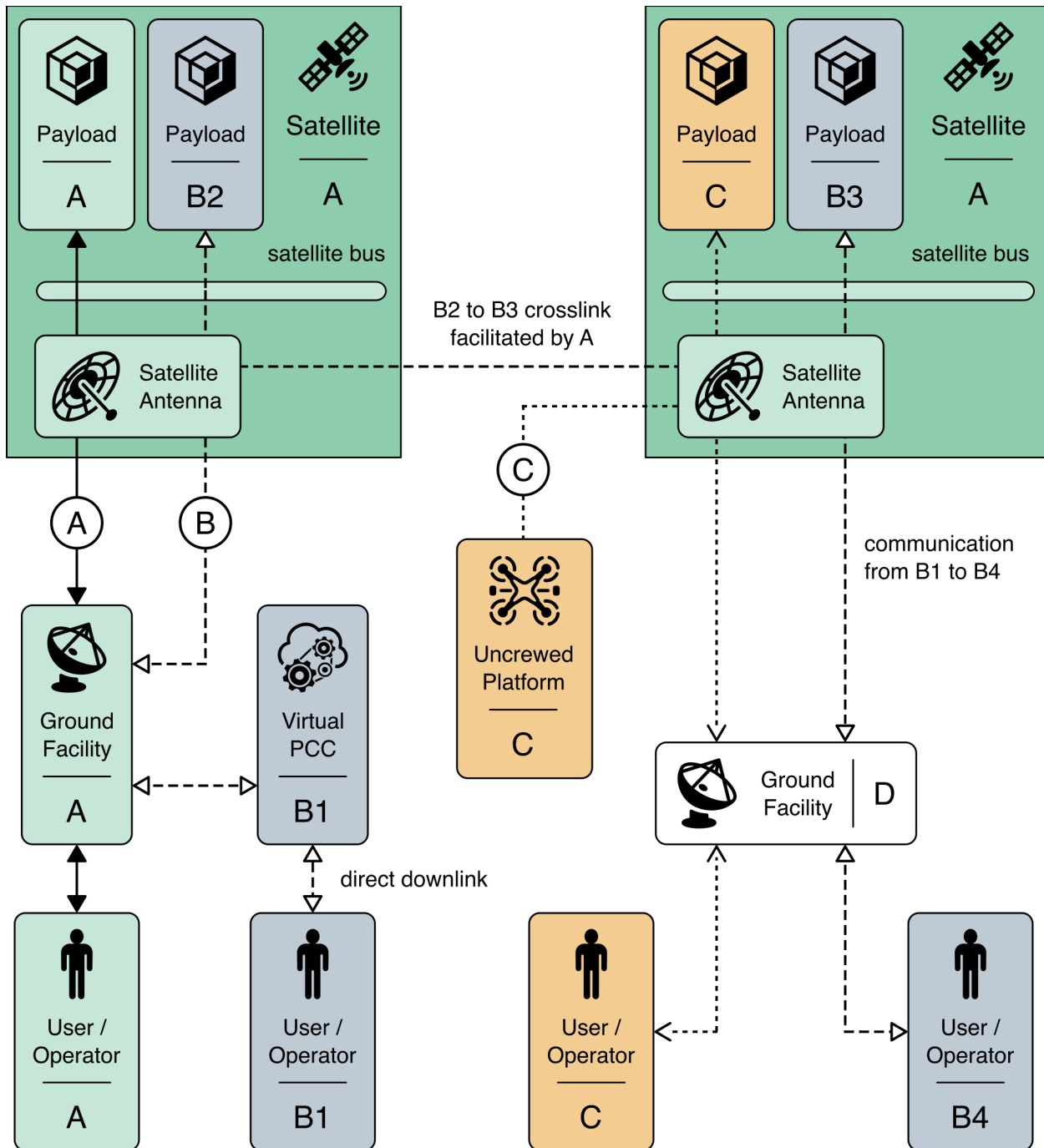
Fig. 3. Example of more complex HSN architecture.

HSN architectures may be complex and involve multiple stakeholders. As shown in Fig. 3, the physical and virtual architecture involves multiple independently owned satellites, uncrewed platforms, ground facilities and crosslinks supporting a range of independent HSNs. The organization that owns and operates the host (A) is supporting two independent HSNs (B and C). The operators associated with HSN B interface with a virtual payload command center that controls payloads on separate satellites. The crosslink and RF interfaces are transparent to HSN

275 B. The host organization, A, may interface with other platforms such as uncrewed vehicles or
276 independently owned antenna fields.

277 The scope of the HSN profile focuses on physical and virtual interfaces such as:

278 • Antenna fields

279 • Virtual Machine based command formatter

280 • Software-defined elements hosted on a cloud

281 • Bus

282 • Payloads

283 • User terminals

284 • Intermediate ground nodes

285 • Intersatellite cross links for purposes such as linking to a payload hosted on another
286 satellite, higher resolution, greater communication bandwidth, path redundancy, etc.

287 This HSN profile is intended to:

288 • Facilitate integration of HSN components thorough consideration of cybersecurity
289 functions, categories, and subcategories.

290 • Consistently, assess the cybersecurity posture.

291 • Provide a comprehensive framework to facilitate risk management decisions.

292 • Facilitate consistent assessments of cyber-risk.

293 • Consistently communicate cybersecurity posture and priorities.

294 The HSN profile provides a subset of CSF subcategories that are directly applicable to the HSN
295 and strategies that could be implemented. The HSN profile allows each organization the
296 flexibility to implement selected mitigation strategies based on their risk tolerance or accepted
297 risk management strategy.

298 The HSN profile will focus on the complex variety of interfaces, data flows, and interactions
299 with third-party services or component providers involved in modern HSNs. Many of these
300 systems require connections to external partners or entities that are not trusted. Interfacing with
301 untrusted systems requires the individual systems to understand and bound the inherited risk and
302 ensure their confidentiality, integrity, and availability. The HSN profile will address concerns
303 unique to HSN and the reader is referred to other CSF profiles to address space system segments
304 or components that are beyond this profile's scope.

305 **1.3. Audience**

306 This document is intended for those involved in managing, developing, implementing, and
307 monitoring the HSN cybersecurity including:

308 • Procurement officials responsible for the acquisition of HSN services

309 • Public and private organizations that provide HSN services

310   • Managers responsible for the use of HSN services

311   • Risk managers, cybersecurity professionals, and others with a role in cybersecurity risk
312   management for systems that provide or interface with HSN services

313   • Mission and business process owners responsible for achieving operational outcomes
314   dependent on HSN services

315   • Researchers and analysts who study the unique cybersecurity needs of HSN services

316   • Cybersecurity architects who integrate cybersecurity into the product designs for space
317   vehicle segments and ground segments

2. Intended Use

319   This profile is part of an overall risk management strategy for satellites operating in hybrid
320   environments. The intent is to provide actionable practical guidance to assess current posture and
321   inform future decisions.

322   Decision makers are tasked with determining acceptable risk and this CSF profile is a tool to
323   help inform decision-makers concerning potential risks. Capabilities and priorities can be set
324   using an enhanced cybersecurity posture. This CSF profile provides an HSN-specific framework
325   that facilitates assessments of the cybersecurity posture of the HSN and can be used as part of a
326   larger security in-depth assessment for the space system. The CSF profile is intended to augment,
327   not replace, the organization's risk management procedures.

328   NIST recognizes that the HSN profile will be applied to specific organizations with specific
329   needs. To this end, a summary of considerations for customization is provided below.

330   • Operational considerations

331   ○ What methods can be used to detect potential events of concern?

332   ○ What methods can be used to respond to the detected events?

333   ○ What methods can be employed for post-event recovery?

334   • Mission considerations

335   ○ What services are mission-critical?

336   ○ What systems and data/assets are vulnerable?

337   ○ What recovery/fail-over strategies can be employed?

338   ○ What measures are available to determine the effectiveness of security controls?

339   • Engineering Considerations

340   ○ What are the capabilities of the system?

341   ○ What are the capabilities of potential adversaries to the system?

342   ○ Which system attributes are adjustable post-deployment, and which are
343   immutable?

344   • External considerations

345   o   What external systems and data are critical?

346   o   What are the impacts of degraded or failed external services?

3. Overview

348 This section contains an overview of risk management and the NIST CSF. A profile provides
349 information on risk management and applies the NIST CSF to assist with specific security
350 implications. The HSN profile will include informative references to existing standards,
351 guidelines, and best practices.

3.1. Risk Management Overview

353 Risk management is the ongoing process of identifying, assessing, and managing the residual
354 risk related to an organization's objectives. To manage risk, organizations should understand the
355 likelihood of an event and its potential impacts. With this information, the acceptable level of
356 risk to the data and services can be determined.

357 As an organization analyzes its objectives as they relate to reliance on or use of HSNs, there are
358 a series of guiding questions that inform the process to include:

359   • What are the threats to achieving mission objectives?
360   • What damages can result when those mission objectives are disrupted?
361   • What are the most important assets for a given mission objective?
362   • Where does physical infrastructure affect cybersecurity infrastructure and vice versa?

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

366 The profile supports and is informed by cybersecurity risk management processes. Using the
367 profile, organizations can make more informed decisions to select and prioritize cybersecurity
368 activities and expenditures that help identify systems dependent on HSN, identify appropriate
369 HSN sources, detect disturbances and manipulation of HSN services, manage the risk to these
370 systems, and bolster resilience. The HSN profile provides a starting point from which
371 organizations can customize—based on need and risk tolerance—to develop the most
372 appropriate processes to manage cybersecurity posture of their HSN.

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

3.2. Cybersecurity Framework Overview

379 Created through collaboration between industry and government, the Cybersecurity Framework
380 [NIST-CSF] provides prioritized, flexible, risk-based, and voluntary guidance based on existing

381 standards, guidelines, and practices to help organizations better understand, manage, and
382 communicate cybersecurity risks.

383 The Cybersecurity Framework consists of three main components:

384   1. The Framework Core provides a catalog of desired cybersecurity activities and outcomes
385   using common language. The Core guides organizations in managing and reducing their
386   cybersecurity risks in a way that complements their existing cybersecurity and risk
387   management processes.
388   2. The Framework Implementation Tiers provide context for how an organization views
389   cybersecurity risk management. The Tiers help organizations understand whether they
390   have a functioning and repeatable cybersecurity risk management process and the extent
391   to which cybersecurity risk management is integrated with broader organization risk
392   management decisions.
393   3. The Framework Profiles are customized to the outcomes of the Core to align with an
394   organization's requirements. Profiles are primarily used to identify and prioritize
395   opportunities for improving organizational cybersecurity.

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

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

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

418 The Framework Core then identifies underlying Categories and Subcategories for each Function.
419 The 108 Subcategories are discrete cybersecurity outcomes that are organized into 23 Categories,
420 such as "Asset Management" and "Protective Technology". Fig. 4 depicts the basic structure of
421 the Framework Core.

Fig. 4. Structure of the Framework Core.

423 The Cybersecurity Framework is outcome-based and focuses on the cybersecurity functions
424 rather than the components. A Cybersecurity Framework Profile is not intended to provide
425 specific implementation guidance. However, a Profile will supply Informative References to
426 existing standards, guidelines, and practices that provide practical guidance to help an
427 organization achieve the desired outcome of each Subcategory. An example of two
428 Subcategories and their Informative References within the Asset Management Category is shown
429 in Fig. 5.

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

Fig. 5. Cybersecurity Framework Subcategory Example.

431 A Cybersecurity Framework Profile is an assessment of an organization in the context of the
432 Cybersecurity Framework Core. A "current" Profile is a review of the Core Subcategories in
433 terms of their applicability and current efficacy from the organization's perspective. A "target"
434 Profile is a set of Subcategories that an organization selects as being relevant to achieving the
435 desired cybersecurity state. A gap is identified when a target Subcategory is missing or
436 insufficiently implemented by the current Profile.

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

439 **4. The HSN CSF Profile**

440 This section was created using the Cybersecurity Framework, as described in <u>Sec. 3.2</u>. The tables
441 summarize the Subcategories within a Category for a Function. The Informative References
442 provide additional guidance to aid risk management practitioners when applying this profile.

443 While reviewing the tables presented in Sec. 4.1–4.5 of this profile, the term "organization"
444 refers to the entity that is an element of the HSN and is assessing their cybersecurity posture. All
445 other elements of the HSN are referred to as partners, stakeholders, service providers, or external
446 organizations.

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

452 **4.1. Identify**

453 The Identify Function is foundational to cybersecurity and the risk management process.
454 Cybersecurity assessments and risk management should start with the Identify Function.
455 Consideration of the organization's mission and business objectives, threat environment, assets,
456 and vulnerabilities will have a significant influence on the overall risk management decision and
457 will impact the other four Functions (i.e., Protect, Detect, Respond, Recover).

458 The objectives of the Identify Function include:

459 • Identify the business or operational environment and organization's purpose.

460 • Identify all assets, including hardware, software, personnel, roles, responsibilities, and the
461 assets' criticality.

462 • Identify infrastructure that provides HSN functionality.

463 • Identify the current and trending vulnerabilities, threats, and impacts should the threat be
464 realized.

465 The Identify Function within the CSF defines six Categories which are summarized in the
466 following subsections below: Asset Management, Business Environment, Governance, Risk
467 Assessment, Risk Management Strategy, and Supply Chain Risk Management. Each Category
468 has at least one Subcategory that directly applies to HSN.

469 **4.1.1. Asset Management Category**

470 The data, personnel, devices, systems, and facilities that enable the organization to achieve its
471 business objectives are identified and managed in a manner that is consistent with their
472 importance to organizational objectives and the organization's risk strategy.

473 Asset management and prioritization are important factors in other functions and activities, such
474 as contingency planning for future attacks, responding to malware events, emergency responses,

475 and recovery actions. Asset management will assist in prioritizing response and recovery
476 activities.

477 In the context of HSNs, inventory internal and external devices and their configurations.
478 Working knowledge of the interfaces and data flows between devices and organizations
479 respectively will illuminate areas of risk and needed protective measures.

480 The Identify asset management category has six subcategories that applies to HSNs.

481 **Table 1.** Asset Management Category for the Identify Function.

Identify Asset Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.AM-1: Physical Devices and systems within the organization are inventoried.	Focus on the interfaces of the physical devices that interact with external organizations Need to have a working knowledge of the physical systems owned vs leased by external organizations as well as any constraints, performance requirements, and tolerances to successfully interface. Collaboration with external organizations is necessary to execute a physical inventory that spans organization locations and ownership. HSNs must be aware that there are limits on the ability to execute a physical inventory (relative to an internal inventory).	**NIST SP 800-53r5** CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried.	Focus on the interface between organizations. Understand software configurations and version control to ensure interoperability (internal and external). Typically, HSNs have a large and dynamic inventory. Understand the limitations associated with complex	**NIST SP 800-53r5** CM-8, PM-5

Identify Asset Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	inventory processes and procedures. Consider some level of automation.	
ID.AM-3: Organizational communication and data flows are mapped.	Ensure only necessary data is sent or received to fulfill the mission. Verify data sources and recipients are authorized to send or receive data. Flows may originate (and terminate) from (and to) very different nodes such as a satellite, a terrestrial terminal, an operations center, an Unmanned Aerial System, or another platform. In addition to the logical data flows, HSNs need to map physical ports/ interfaces and document whether it is a common bus or somehow segregated.	**NIST SP 800-53r5** CA-3, CA-6, CA-9, PM-10, PL-8, SA-17, AC-20
ID.AM-4: External information systems are cataloged.	Applicable, no HSN-specific considerations.	**NIST SP 800-53r5** AC-20, PM-5, SA-9
ID.AM-5: Resources (e.ge., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	Prioritization of internal and external assets informs risk assessment. Emphasize data and services provided externally. The HSN's prioritization effort should include third-party relationships, agreements, and understandings between the participants.	**NIST SP 800-53r5** SA-9, CP-2, AC-20, RA-2, RA-9, SA-20, SC-6
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	All participating organizations should assign cybersecurity roles and be responsible for the software, data, and/or components they manage. The roles and	**NIST SP 800-53r5** SA-9, CP-2, PM-2, PM-29, PS-7 **ETSI TR 101 984** 5.2

Identify Asset Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	responsibilities of the external organization to the HSN need to be agreed upon in advance. Identify and resolve any inconsistencies or gaps in advance.	

4.1.2. Business Environment Category

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

In the context of HSNs, identify the dependencies, obligations, and relationships between different organizations and their stakeholders to resolve any differences.

The Identify business environment category has five subcategories that apply to HSNs.

Table 2. Business Environment Category for the Identify Function.

Identify Business Environment		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.BE-1: The organization's role in the supply chain is identified and communicated.	Identify the role in the supply chain and consider the partners' role in the supply chain. Clearly communicate any corresponding expectations and requirements.	**NIST SP 800-53r5** SR-1, SR-3 **NIST SP 800-161**
ID.BE-2: The organization's place in critical infrastructure and its industry sector are identified and communicated.	Placement in critical infrastructure is based on the service(s) provided (e.g., Communication services, Emergency services, etc.). The determination of critical may be mission specific, orbit-specific or system specific. Understand the role in the critical infrastructure of partner organizations and the	**NIST SP 800-53r5** PM-8 **PPD-21**

Identify Business Environment		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	corresponding expectations. Capture the partner's requirements in addition to what will be provided to fulfill the operational objectives.	
ID.BE-3: Priorities for organizational missions, objectives, and activities are established and communicated.	The HSN implementation and operation must prioritize the mission objectives to establish performance and evaluate service providers.	**NIST SP 800-53r5** PM-11
ID.BE-4: Dependencies and critical functions for the delivery of critical services are established.	HSNs that rely on function from external service providers critical to operations are classified as such. Identify dependencies between organizations (hardware, software, data) to successfully define and execute the tasks.	**NIST SP 800-53r5** PM-8, RA-9, SA-20,
ID.BE-5: Resilience requirements to support the delivery of critical services are established.	Especially important for HSNs to provide for the resiliency requirements critical to the HSN (operations or mission). Any Memorandum of Understanding (MOU) or Service Level Agreement (SLA) should spell out performance and resilience requirements in advance. Resilience requirements must be unambiguous so that the minimum performance parameters of service providers (to the HSN) can be defined.	**IEC 61850-90-4** 12.2, 14.2.4 **NIST SP 800-53r5** CP-2, CP-11, CP-12, CP-13, SA-8 **3GPP TR 38 811** 5

490   ### 4.1.3. Governance Category

491   The policies, procedures, and processes to manage and monitor the organization's regulatory,
492   legal, risk, environmental, and operational requirements are documented, reviewed, and inform
493   the management of cybersecurity risk.

494   The Identify governance category has four subcategories that apply to HSNs.

495   **Table 3.** Governance Category for the Identify Function.

Identify Governance		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.GV-1: Organizational cybersecurity policy is established and communicated.	Identify key functions and assign areas of responsibility (to include service providers and external organizations) to ensure a comprehensive cybersecurity approach. Capture the policy requirements for the mission data and payloads, then apply policy and controls appropriately.	**NIST SP 800-53r5** AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	Establish agreements in advance to define roles and responsibilities with any third-party to fulfill the pre-defined policies and performance parameters. (Refer to ID.BE-1, ID.BE-3, and ID.AM-6)	**NIST SP 800-53r5** PM-1, PM-2, PM-29, PS-7, PS-9
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Privacy and civil liberty concerns are typically addressed within the organization (and beyond the control of the external organizations that provide HSN component/service providers).	**NIST SP 800-53r5** AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1
ID.GV-4: Governance and risk management processes address cybersecurity risks.	Within an HSN, there will be varying levels of risk management rigor for different cybersecurity related	**NIST SP 800-53r5** PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2

Identify Governance		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	components such as data vs bus vs payloads.	**NIST SP 800-160V1** 3.3.8

4.1.4. Risk Assessment Category

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

The HSN elements may have varying risk tolerance levels, and the HSN may inherit a level of risk from its partners or other components of the HSN that exceeds its risk tolerance. Identify cyber risks associated with external service providers and their components as it relates to the overall risk management strategy.

The Identify risk assessment category has six subcategories that apply to HSNs.

Table 4. Risk Assessment Category for the Identify Function.

Identify Risk Assessment		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.RA-1: Asset vulnerabilities are identified and documented.	In addition to traditional vulnerability management, HSN systems need to focus on the interfaces and be aware of vulnerabilities inherited from the external service provider.	**NIST SP 800-53 Rev. 5** CA-2, CA-5, CA-7, CA-8, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources.	Applicable, no HSN-specific considerations.	**CISA-ICS** **DHS-NCCIC** **NIST SP 800-53 Rev. 5** PM-15, PM-16, RA-10, SI-5 **NIST SP 800-150**
ID.RA-3: Threats, both internal and external, are identified and documented.	Applicable, no HSN-specific considerations.	**DIA-SPACE**

Identify Risk Assessment		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
		NASIC **NISTIR 8179** **NIST SP 800-37 Rev. 2** **NIST SP 800-53 Rev. 5** PM-12, PM-16, RA-3, RA-10, SI-5 **NIST SP 800-154** **NIST SP 800-160 Vol. 1** 2.3 **RTCA-DO-235** 4-12 **3GPP TR 38_811** 5.3, 6.6 [**Li 2020**]
ID.RA-4: Potential Business impacts and likelihoods are identified.	In addition to impacts/likelihood to the HSN, understand the impact/likelihood to partner organizations or HSN service providers and consider any corresponding impact on Memorandum of Agreement (MOA), MOU, SLA or similar document.	**NIST-SP800-53 Rev. 5** CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 **RTCA-DO-235** 2.1, 13
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Applicable, no HSN-specific considerations.	**IETF-RFC8915** 3-9 **NIST SP 800-30 Rev. 1** **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-16, PM-28, RA-2, RA-3 **NIST-SP800-160V1** 2.3, 2.4 **RTCA-DO-235** 2.1-2.4, 3, 14

Identify Risk Assessment		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
		3GPP TR 38.811
ID.RA-6: Risk responses are identified and prioritized.	Understand how a risk response may impact a partner organization or HSN component/service providers. The prioritization should be informed by the impact of the response (to the external organization) which could result in a possible failure to fulfill a partner agreement/contract element.	**NIST SP 800-53 Rev. 5** CA-5, PM-4, PM-9, PM-28, RA-7

4.1.5. Risk Management Category

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

In the context of HSNs, the risk management strategy must be informed by the tolerances and constraints of the contributing organizations. A level of collaboration and negotiation will be required across the partners to ensure a consistent and compatible set of risk management processes and procedures.

The Identify risk management category has three subcategories that apply to HSNs.

Table 5. Risk Management Category for the Identify Function.

Identify Risk Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	In addition to the organizational stakeholders, an agreement between the HSN, its partners, and providers is beneficial if a collaborative effort is needed to mitigate an attack, vulnerability, or otherwise manage the residual risk.	**NIST SP 800-53 Rev. 5** PM-9, PM-28

Identify Risk Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	In addition to intra organizational segmentation and risk management, the HSN's risk tolerance must be determined and clearly expressed as performance parameters. Performance parameters can be communicated to external component and service providers as requirements.	**NIST SP 800-53 Rev. 5** PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** PM-8, PM-9, PM-11, RA-9

4.1.6. Supply Chain Risk Management

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.

Supply chain risk management (SCRM) is typically an intra-organization function. In the context of HSNs, organizations will need to understand the partner's SCRM so that the impacts of any risk inherited by partners is understood and within the level of the organization's tolerance.

The Identify supply chain risk management category has five subcategories that apply to HSNs.

Table 6. Supply Chain Risk Management Category for the Identify Function.

Identify Supply Chain Risk Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.SC-1: Cyber supply chain risk management processes are identified established, assessed, managed, and agreed to by organizational stakeholders.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** PM-30, SA-9, SR-1, SR-2, SR-3, SR-5 **NIST SP 1800-161**

Identify Supply Chain Risk Management		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6 **NIST SP 800-161** 2.2, 3
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** SA-4, SA-9, SR-2, SR-3, SR-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.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, PS-7, SA-9, SA-11
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** CP-2, CP-4, IR-3, IR-4, IR-8, IR-9

4.2. Protect

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

529 The objectives of the Protect Function include:

530 • Protecting the systems that format and transmit information to the elements of the HSN at
531 the required level of assurance.

532 • Protecting the systems that receive and process data from independent organizations
533 within the HSN.

534 • Should a threat be realized, protect users and applications that depend on HSN data by
535 enabling them to maintain a sufficient level of operations through verified response and
536 recovery plans.

537 The Protect Function defines six Categories summarized in Table 2: Access Control, Awareness
538 and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and
539 Protective Technology. Each of these Categories has at least one Subcategory that applies to
540 HSN.

4.2.1. Protect: Identity Management, Authentication, and Access Control

542 Access to physical and logical assets and associated facilities is limited to authorized users,
543 processes, and devices. These assets are managed in a manner consistent with the assessed risk
544 of unauthorized access to authorized activities and transactions.

545 Relative to other organizations, HSNs will need to provide greater access to external
546 organizations to function. Organizations should consider more granular levels of identity
547 management, authentication, and access controls balance limiting exposure and allowing
548 sufficient access so that the partner's function can be supplied.

549 The Protect identity management, authentications and access control category has seven
550 subcategories that apply to HSNs.

551   **Table 7.** Identity Management, Authentication and Access Control Category for the Protect Function.

| Protect | | |
Identity Management, Authentication and Access Control		
Subcategory	**Applicability to HSNs**	**References**
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	Emphasize managing credentials of devices, users, and processes identified by external organizations.	**NIST SP 800-63-3** **NIST SP 800-207** **NIST SP 800-53 Rev. 5** IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12
PR.AC-2: Physical access to assets is managed and protected.	Emphasize managing physical access to assets by external organizations.	**NISTIR 8320** **NIST SP 800-53 Rev. 5** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9

Protect		
Identity Management, Authentication and Access Control		
Subcategory	**Applicability to HSNs**	**References**
PR.AC-3: Remote access is managed.	Critical for HSNs. In addition to remote for normal operations, remote access will need to be granted to external operators, users, and other personnel. Agile remote access procedures will need to be in place in accordance with the agreements between partners' and the organization's contingency plans.	**NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed incorporating the principles of least privilege and separation of duties.	Given the necessity for external entities to interact with the HSN, highly granular authorizations are needed to accommodate the principles of least privilege and separation of duties to limit the impact of potential damage from a particular entity.	**NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 **NIST SP 800-160 Vol. 1** Appendix F.1.14
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	HSNs have a potentially large attack surface due to lack of direct control over external organizations. Measures such as network segmentation, isolation of flows, etc., are essential for containing the damage.	**NIST SP 800-207** **NIST SP 800-53 Rev. 5** AC-4, AC-10, SC-7, SC-10, SC-20
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	Third-party roots of trust or certificate authority credential organizations agreed upon by the HSN participants are beneficial.	**NIST SP 800-63-3** **NIST SP 800-53 Rev.5** AC-16, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10

Protect Identity Management, Authentication and Access Control		
Subcategory	**Applicability to HSNs**	**References**
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).	Establish procedures and controls to authenticate external entities before allowing connections. Given the possibility of many external participants not under the direct control of the organization, preventing unauthenticated communication should be a high priority. Evaluate the risks and implement adequate controls in accordance with the diversity of the HSN. Consider controls such as multi-factor authentication.	**NIST SP 800-53 Rev. 5** AC-16, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10

4.2.2. Protect: Awareness and Trainings Category

The organization's personnel and partners are provided cybersecurity awareness education and trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

The awareness and training category is not unique to HSN or the satellite industry. The focus on privileged users who operate, monitor, and maintain equipment that interfaces with the organization and third-party partners. Within an HSN, third-party and partner relationships vary widely and are coordinated in advance.

The Protect awareness and trainings category has five subcategories that apply to HSNs.

Table 8. Awareness and Trainings Category for the Protect Function.

Protect Awareness and Trainings		
Subcategory	**Applicability to HSNs**	**References**
PR.AT-1: All users are informed and trained.	HSN operators should ensure staff receives adequate cybersecurity training, especially on assets not internal to the organization.	**NIST SP 800-53 Rev. 5** AT-2, PM-13, PM-14

Protect Awareness and Trainings		
Subcategory	**Applicability to HSNs**	**References**
PR.AT-2: Privileged users understand their roles and responsibilities.	Consider providing more specialized training to HSN personnel for the bus and payload in accordance with the granularity of the authorization and operation policies.	**NIST SP 800-53 Rev. 5** AT-3, PM-13 **NIST SP 800-160 Vol. 2 Rev. 1** Appendix E
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	Establish agreements regarding third-party roles and responsibilities in advance.	**NIST SP 800-53 Rev. 5** AT-3, PS-7, SA-9
PR.AT-4: Senior executives understand their roles and responsibilities.	The HSN will require shared usage across the elements of the HSN. Senior executives from the different organizations will need to agree upon and ensure buy-in within their organization so that the terms of the agreements will be met.	**NIST SP 800-53 Rev. 5** AT-3, PM-13
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** AT-3, CP-3, IR-2, PM-13

4.2.3. Protect: Data Security Category

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

External partners may provide HSN data protection requirements or the HSN may have an obligation to provide data security for partner organizations. The tools, techniques, processes, and procedures will require a level inter-organization access and cooperation that other organizations do not typically encounter.

The Protect data security category has eight subcategories that apply to HSNs.

Table 9. Data Security Category for the Protect Function.

Protect Data Security Category		
Subcategory	**Applicability to HSNs**	**References**
PR.DS-1: Data at rest is protected.	HSNs should consider data at rest protection in accordance with data retained by external organizations. Protection measures should correlate with sensitivity. Data encryption and storage measures should be communicated and written into policy.	**NIST SP 800-37 Rev. 2** 3 **NIST SP 800-53 Rev. 5** MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 **NIST-SP800-175B Rev. 1** **NIST SP 800-209**
PR.DS-2: Data in transit is protected.	Data encryption and decryption practices should be discussed with external organizations. Consider measures such as error detection, error correction, bulk link encryption and other transport layer protections. Given that Radio Frequency (RF) is the satellite's main communication conduit, availability protection measures such as Direct Sequence Spread Spectrum or Frequency Hopping Spread Spectrum should be considered.	**NIST SP 800-53 Rev. 5** SC-8, SC-11, SC-12
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	Policies and methods for managing removal, transfers, and dispositions between internal and external assets maintain confidentiality and integrity.	**NIST SP 800-53 Rev. 5** CM-8, MP-6, PE-16, PE-20
PR.DS-4: Adequate capacity to ensure availability is maintained.	In addition to the availability requirements for the organization's business needs, determine	**NIST SP 800-53 Rev. 5** AU-4, CP-2, PE-11, SC-5

Protect		
Data Security Category		
Subcategory	Applicability to HSNs	References
	what level of availability needs to be maintained in accordance with the requirements of the partner organizations.	
PR.DS-5: Protections against data leaks are implemented.	Shared information between organizations should follow policies on data handling to reduce the potential for data leaks.	**NIST SP 800-53 Rev. 5** AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** SI-7, SI-10 **NIST SP 800-160 Vol. 1** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F **NIST SP 800-161** **NIST SP 800-193** **NIST SP 800-218** PO.3.3, PS.1
PR.DS-7: The development and testing environments are separate from the production environment.	Not directly applicable to HSN.	**FIPS 140-3** **NISTIR 8320** **NIST SP 800-53 Rev. 5** SA-10, SI-7 **NIST SP 1800-34**
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	Verify the integrity of the hardware required to make the HSN system operational. Implementors need to be aware of challenges associated with verifying hardware built by different vendors. Consider the use of independent assessors or third-party verification	**FIPS 140-3** **NISTIR 8320** 4 **NIST SP 800-53 Rev. 5** SA-10, SI-7 **NIST SP 1800-34**

Protect		
Data Security Category		
Subcategory	**Applicability to HSNs**	**References**
	during the operational phase.	

4.2.4. Protect: Information Protection Processes and Procedures Category

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to protect information systems and assets.

In the context of HSNs, security policies must be coordinated among external partners and stakeholders in addition to internal entities.

The Protect information protection processes and procedures category has twelve subcategories that apply to HSNs.

Table 10. Information Protection Processes and Procedures Category for the Protect Function.

Protect		
Information Protection Processes and Procedures		
Subcategory	**Applicability to HSNs**	**References**
PR.IP-1: A baseline configuration of information technology/industrial control systems is created, maintained, and incorporates security principles (e.g., concept of least functionality).	Focus on the configuration and maintenance of the entities at the interface to the HSN. Baseline and configuration are internal concerns and obtaining detailed configuration information from the partners is not practical.	**NIST SP 800-53 Rev. 5** CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 **NIST SP800-137** Section D **NIST SP800-160V1** 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G
PR.IP-2: A System Development Life Cycle to manage systems is implemented.	System Development Life Cycle is an internal responsibility and third-party components are evaluated prior to integration with the system. The HSN should provide guidance on what may or may not be integrated with the HSN.	**NIST SP 800-53 Rev. 5** SA-3, SA-4, SA-8, SA-10, SA-11 **NIST SP800-137** Section D **NIST SP800-160V1** 3.3.5, 3.8.3, 3.8.4
PR.IP-3: Configuration change control processes are in place.	Organizations should employ configuration change control consistent with the software	**NIST SP 800-53 Rev. 5** CM-3, CM-4, SA-10 **NIST SP 800-137** Section D

Protect		
Information Protection Processes and Procedures		
Subcategory	**Applicability to HSNs**	**References**
	development life cycle to maintain a functioning baseline for the HSN and its components. Monitor all changes to validate impacts and integrity and conduct impact analyses before deploying a change.	**NIST SP 800-160v1** 3.3.5, 3.8.3, 3.8.4
PR.IP-4: Backups of information are conducted, maintained, and tested.	Usually an internal function, however, is highly dependent on the service provided by the partner.	**NIST SP 800-53 Rev. 5** CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	Applicable to HSN and complicated by 3rd party owned components (hardware, software, applications, etc.) No HSN-specific concerns.	**NIST SP 800-53 Rev. 5** PE-1
PR.IP-6: Data is destroyed according to policy.	Ensure data retained by third parties are disposed of properly. Likewise, external organizations should ensure data no longer required for HSN operations are destroyed according to pre-arranged agreements and policies.	**NIST SP 800-53 Rev. 5** MP-6, SR-12
PR.IP-7: Protection processes are improved.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6
PR.IP-8: The effectiveness of protection technologies is shared.	Effectiveness of protection technologies are shared with partner organizations in a manner that is consistent with pre-existing agreements while protecting the organization's equities.	**NIST SP 800-53 Rev. 5** AC-21, CA-7, CP-2, IR-8, SI-4 **NIST SP800-150**

Protect		
Information Protection Processes and Procedures		
Subcategory	**Applicability to HSNs**	**References**
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Creating and managing these plans is complicated by the diversity of the partners information, geographic separation, and complicated interfaces.	**IEC 61850-90-12** 5.8, 4.12-4.14 **NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9, PE-17 **NIST SP800-61 Rev. 2** **NIST SP800-160V1** 6.5, 6.6, Appendix F.2
PR.IP-10: Response and recovery plans are tested.	HSNs need to include the partner organizations when testing response and recovery plans. Full-scale tests involving the partners requires significant effort and coordination. Given the level of effort (and corresponding costs), modeling and simulation of the partners participation in the test may be the only pragmatic approach.	**IEC61850-90-4** 14.2.4, 5.4.2.5 **NIST SP800-53r5** CP-4, IR-3, PM-14 **NIST SP800-115**
PR.IP-11: Cybersecurity is included in human resources in practices (e.g., deprovisioning, personnel screening).	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21
PR.IP-12: A vulnerability management plan is developed and implemented.	Develop and implement a vulnerability management plan. A vulnerability management plan that addresses managing vulnerabilities that are potentially inherited from external organizations and assets will be necessary.	**NIST SP 800-53 Rev. 5** RA-1, RA-3, RA-5, SI-2

580 **4.2.5. Protect: Maintenance Category**

581 Maintenance and repairs of industrial control and information system components are performed
582 consistently with policies and procedures.

583 The policies and procedures that pertain to maintenance and repairs within the HSN should be
584 agreed upon in advance across the elements of the HSN.

585 The Protect maintenance category has two subcategories that apply to HSNs.

586 **Table 11.** Maintenance Category for the Protect Function.

Protect Maintenance		
Subcategory	**Applicability to HSNs**	**References**
PR.MA-1: The maintenance and repair of organizational assets are performed and logged with approved and controlled tools.	Directly applicable for firmware and software considerations, but not directly applicable to other assets.	**NIST SP 800-53 Rev. 5** MA-1, MA-2, MA-3, MA-5, MA -6
PR.MA-2: Remote maintenance of organizational asset is approved, logged, and performed in a manner that prevents unauthorized access.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** MA-4 **NIST SP 800-160V1** Appendix F.1.14

4.2.6. Protect: Protective Technology Category

588 Technical security solutions are managed to ensure the security and resilience of systems and
589 assets consistent with related policies, procedures, and agreements.

590 HSNs require collaboration and cooperation. Organizations should consider using protective
591 technologies with standardized interfaces, formats, and protocols to facilitate collaboration and
592 ensure compatibility.

593 The Protect protective technology category has five subcategories that apply to HSNs.

594 **Table 12.** Protective Technology Category for the Protect Function.

Protect Protective Technology		
Subcategory	**Applicability to HSNs**	**References**
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	Promote standardized event record formats across organizations for easy sharing and event analysis. Consideration should be given to policies that promote audit log sizing,	**NIST SP 800-53 Rev. 5** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU- 16

Protect Protective Technology		
Subcategory	Applicability to HSNs	References
	and aging that meet industry best practices.	
PR.PT-2: Removable media is protected, and its use is restricted according to policy.	HSNs may need to support using removable media to exchange data between partners and other organizations.	**NIST SP 800-53 Rev. 5** MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Limit the data exchanges and functionality between the organization and the partners as much as practical while maintaining the HSN's mission needs.	**NIST SP 800-53 Rev. 5** AC-3, CM-7
PR.PT-4: Communications and control networks are protected.	Ensure that multiple organizations sharing common infrastructure have proper controls to meet organizational policies.	**NIST SP 800-53 Rev. 5** AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC- 31, SC-37, SC-38, SC-47
PR.PT-5: Mechanism (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	Consider load balancing mechanisms such as alternate data/ service sources in addition to other resiliency measures.	**NIST SP 800-53 Rev. 5** CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6

4.3. Detect

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

The objectives of the Detect Function include:

- Enabling detection through monitoring and consistency checking

- Establishing a process for deploying detection capabilities and the handling/disposition of detected anomalies and events.

The Detect Function may leverage capabilities such as automation and management tools such as Security Information and Event Management to assist in detecting previously uncovered threats and minimize false positives. These capabilities involved data parsing, analytics, and the sharing

606 of information. In an HSN environment, all the data message formatting and transmission must
607 be compatible. If practical, comply with standards-based solutions for data formatting, message
608 formatting, and message transmission to facilitate interoperability, integration, and sharing.

4.3.1. Detect: Anomalies and Event Category

610 Anomalous activity is detected, and the potential impact of events is understood.

611 HSNs may need to detect anomalous activity and perform analysis on behalf of a partner or,
612 conversely, rely on external organizations for detection and analysis.

613 The Detect Anomalies and Event category has five subcategories that are apply to HSNs.

614 **Table 13.** Anomalies and Event Category for the Detect Function.

Detect Anomalies and Event		
Subcategory	**Applicability to HSNs**	**References**
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	In the context of HSNs, it is especially important to focus on the expected (or normal) data and information flows at the ingress and egress of the interfaces (including wired, RF and virtual). Verify operational performance baselines and expected data flows between the elements of the HSN are captured, developed, and maintained at the appropriate interfaces to detect events.	**NIST SP 800-53 Rev. 5** AC-4, CA-3, CM-2, SC-16, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	Review and analyze detected events within the HSN system in (i) real time to maintain normalcy of operations; and (ii) forensically to understand the characteristics (e.g., source, data error statistics, duration, frequency, and location) of anomalous events. Be able to identify potential cyber incidents and understand attack targets and methods.	**NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, RA-5, SI-4

Detect Anomalies and Event		
Subcategory	**Applicability to HSNs**	**References**
	Be able to distinguish between potentially harmful events and normal operations. Be able to predict the level of harm based on event analysis. Use a common methodology agreed upon by stakeholders to facilitate sharing. For RF interference, include environmental monitoring with direction, finding capabilities to locate the source. Preserve the raw data, analysis, and characterization to aid in the analysis of future events. Emphasize insider attacks due to the access granted to external participants and partner organizations within the HSN.	
DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	Data from multiple sources that may be used, cross-checked, and compared to detect anomalous behavior. Compile sufficient event data across the different participants using various sources, such as event reports, logs, audit monitoring, network monitoring, physical access monitoring, environmental monitoring, and human-machine interface user and administrator reports. Standards-based data formatting and serialization	**NIST SP 800-53 Rev. 5** AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 **NIST-SP 800-160V1** 3.3.7, Appendix G.2, Appendix G.3

Detect Anomalies and Event		
Subcategory	**Applicability to HSNs**	**References**
	promotes communication, interoperability, and interchangeability of HSN data and supporting data. Correlate events and cross-check detected anomalies from the different data and service providers. Consider including events from external and authoritative shared resources (e.g., open source, industry forums, user groups, etc.).	
DE.AE-4: The impact of events is determined.	In addition to the impact on the organization, consider the impact on the data and service providers participating in the HSN.	**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-5, IR-8, SI-4
DE.AE-5: Incident alert thresholds are established.	Discussions regarding the setting and review of thresholds should include external stakeholders. Attributes such as criticality, sensitivity, and tolerance to false positives will vary among different service providers and their assets. Consider and document the required notification or alarm communication time upon nearing and exceeding thresholds.	**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-5, IR-8, SI-4

615 ## 4.3.2. Detect: Security Continuous Monitoring Category

616 The information system and assets are monitored to identify cybersecurity events and verify the
617 effectiveness of protective measures.

618 In addition to internal monitoring, HSNs are likely to monitor external partners and elements of
619 the HSN in accordance with prearranged agreements and commitments.

620 The information systems and assets are monitored to identify cybersecurity events and verify the
621 effectives of protective measures. The granularity of the monitoring and the depth of the analysis
622 are consistent with the findings of the risk assessment (refer to ID.RA-1 through ID.RA-5).

623 The Detect security continuous monitoring category has eight subcategories that apply to HSNs.

624 **Table 14.** Security Continuous Monitoring Category for Detect Function.

Detect		
Security Continuous Monitoring		
Subcategory	**Applicability to HSNs**	**References**
DE.CM-1: The network is monitored to detect potential cybersecurity events.	Heighten system monitoring activities when there is an indication of increased risk to the organization or the service providers. Fuse data from multiple sources. Consider using fault detection and exclusion algorithms to analyze data. Alert the participating users and organizations when services or data are unavailable within a specified time agreed upon in advance.	**NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	Not directly applicable to HSNs.	**NIST SP 800-53 Rev. 5** CA-7, PE-6, PE-20
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected.	Given the increased level of access and privileges that may be provided to externally, it is essential to detect malicious code.	**NIST SP 800-53 Rev. 5** SC-44, SI-3, SI-4, SI-8 **NIST SP 800-218**

Detect		
Security Continuous Monitoring		
Subcategory	**Applicability to HSNs**	**References**
	Consider multi-layered detection strategies.	
DE.CM-5: Unauthorized mobile code is detected.	Especially important for HSNs to detect and limit unauthorized mobile code to implement the principles of least privilege and least functionality.	**NIST SP 800-53r5** SC-18, SC-44, SI-4
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Detect deviations from HSN service providers' interface specifications, as defined in an SLA with the service provider.	**NIST SP 800-53 Rev. 5** CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	Focus on data flow discrepancies, unauthorized connections, and access points.	**NIST SP 800-53r5** AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed.	Applicable, no HSN-specific considerations.	**NIST SP 800-53 Rev. 5** RA-5 **NIST SP800-115**

4.3.3. Detect: Detection Processes Category

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

Organizations need a level of awareness for the external partners' testing and maintenance to ensure the processes and procedures are within the HSN's specifications.

The Detect detection processes category has five subcategories that apply to HSNs.

Table 15. Detection Process Category for Detect Function.

Detect		
Detection Processes Category		
Subcategory	**Applicability to HSNs**	**References**
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	All roles—including data collection, analytics, reporting, and notification— are identified, and	**NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14

Detect		
Detection Processes Category		
Subcategory	**Applicability to HSNs**	**References**
	performance criteria are defined when feasible. Understand HSN service provider and sector specific roles and responsibilities. For example, Payload Control Centers (PCC)s responsible for hosted payloads should have an agreement on these roles and responsibilities with the host's Mission Operations Center (MOC) and host satellite.	
DE.DP-2: Detection activities comply with all applicable requirements.	HSNs are likely to have several MOU, SLA, or other agreements. Confirm that detection activities comply with applicable requirements. Organizations with MOCs responsible for hosting third-party payloads should perform detection activities in accordance with predefined agreements for hosted payloads.	**NIST SP 800-53 Rev. 5** AC-1, AU-1, CA-1, CA-2, CA-7, CM-1, CP-1, IR-1, PL-1, PM-1, RA-1, SA-1, SC-1, SI-1, SI-4, SR-1, SR-9, SR-10
DE.DP-3: Detection processes are tested.	Typically, an intra-organization activity. The participating organizations may have agreements in place to test detection processes: however, inter-organization detection processes are atypical.	**NIST SP 800-53 Rev. 5** CA-2, CA-7. PM-14, SI-3, SI-4
DE.DP-4: Event detection information is communicated.	Appropriate responses require event detection information in cyber-relevant time at the HSN interfaces. Thresholds and other criteria must be defined in advance.	**NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA5, SI-4

Detect		
Detection Processes Category		
Subcategory	**Applicability to HSNs**	**References**
	When the cause of a HSN service disruption event is suspected to be external, share event detection with the appropriate external stakeholders for further investigation. Consider sharing detected information with regional Computer Emergency Response Teams or industry organizations, such as Information Sharing and Analysis Centers (ISACs. MOCs with buses that host (or PCCs that are hosted by an independent organization) may have prearranged information sharing agreements.	
DE.DP-5: Detection processes are continuously improved.	Reevaluate the detection processes as the HSN evolves to ensure sufficient robustness. Periodically examine anomaly detection processes to determine if improvements are needed and collaborate with the constituent elements.	**NIST SP 800-53 Rev. 5** CA-2, CA-7, PL-2, PM-14, RA-5, SI-4

632   ## 4.4.   Respond

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

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

639 The objectives of the Response Function are to:

640 • Contain events using a verified response procedure.

641 • Communicate the occurrence and impact of the event on satellite operations and
642 stakeholders.

643 • Develop processes to respond to and mitigate new known or anticipated threats or
644 vulnerabilities.

645 • Evolve response strategies and plans based on lessons learned.

646 **4.4.1. Respond: Response Planning Category**

647 Response processes and procedures are executed and maintained, to ensure response to detected
648 cybersecurity incidents.

649 HSN response planning requires additional efforts to avoid ambiguities. The response plan
650 should be developed and coordinated prior to an incident to ensure that all participants know
651 what can be expected from the HSN and are aware of their obligations.

652 The Respond planning category has a single subcategory that applies to HSNs.

653 **Table 16.** Response Planning Category for Respond Function.

Respond Response Planning		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
RS.RP-1: The response plan is executed during or after an incident.	In accordance with pre-defined thresholds, organizations should coordinate and execute a response plan(s) during or after a cybersecurity event that impacts space systems. Update the response plans to address changes in partners, service providers, and agreements, as well as to the organization itself.	**CISA-CIVR-PB** Appendix B **NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8

654 **4.4.2. Respond: Communications Category**

655 Response activities are coordinated with internal and external stakeholders (e.g., external support
656 from law enforcement agencies).

657 In addition to typical intra-communications required for response activities, organizations need
658 to provide additional consideration to external communications between partners, service
659 providers and other elements of the HSN.

660 The Respond Communications category has five subcategories that apply to HSNs.

661 **Table 17.** Communications Category for Respond Function.

Respond Communications		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
RS.CO-1: Personnel know their roles and order of operations when a response is needed.	Ensure that personnel know, are trained, and have exercised their roles in response to disruptions. Understand the expectations and limitations of the roles provided by external partners and service providers. Responders should understand recovery time objectives, recovery point objectives, restoration priorities, task sequences, and assigned responsibilities for event response programs and processes in a manner that is consistent with business continuity objectives.	**DHS CISA** 1.f, 7.a **DHS RCF** 5.2, 8.3 **IMO** 1575 C.2.2 **NIST SP 800-61** **NIST SP 800-34 Rev.1** 3.2.1, CP-2, CP-3, IR-3, IR-8 **NIST SP 800-53 Rev. 5** CP-2, CP-3, CP-10, IR-3, IR-8 **USG FRP** 5.1.2.5
RS.CO-2: Incidents are reported consistent with established criteria.	Ensure that cybersecurity events which exceed a predetermined threshold are reported across stakeholders.	**DHS-GPS-PR** **NERC** CIP-008-6 **NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8 **NIST SP 800-61 Rev. 2** 4
RS.CO-3: Information is shared consistent with response plans.	Timely information exchange within and between organizations improves the overall efficiency of incident response.	**FCC-JAMMER** **NIST SP 800-53 Rev. 5** AC-21, CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2** 2.4

Respond Communications		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	Exchange information with external stakeholders in accordance with prearranged agreements and thresholds to ensure that obligations are met (see ID.GV-2 and DE.AE-5).	
RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	If the satellite hosts third-party payloads, incidents that impact satellite bus operations should be reported to the stakeholders in accordance with the response plan and prearranged agreements with the PCC (see ID.GV-4).	**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2** 2.4
RS.CO-5: Voluntary information sharing occurs with external stakeholders or achieve broader cybersecurity situational awareness.	Use agreed upon common data formats to facilitate information sharing. Suspected interference should be reported to stakeholders through the appropriate channels and procedures (see DE.DP-4).	**NIST SP 800-53 Rev. 5** PM-15, SI-5

4.4.3. Respond: Analysis Category

662

663 Analysis is conducted to ensure effective response and support recovery activities.

664 An HSN may require analysis from independent groups or elements within the HSN.
665 Organizations should understand the limitations of external analysis reports and determine the
666 appropriate response for a given analytic.

667 The Respond analysis category has five subcategories that apply to HSNs.

668 **Table 18.** Analysis Category for Respond Function.

Respond Analysis Subcategory	Applicability to HSNs	References (HSN-Specific)
RS.AN-1: Notifications from detection systems are investigated.	Investigate cybersecurity-related notifications generated by the anomaly detection systems.	**CISA-CIVR-PB** 10 **CISA-RFI-BPG** **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4
RS.AN-2: The impact of the incident is understood.	Understand impacts that may affect the hybrid user and community, third-party stakeholders (in the case of a MOC that hosts third-party payloads), and/or the end-user community.	**CISA-CIVR-PB** 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3 **NIST SP 800-61 Rev. 2** 3
RS.AN-3: Forensics are performed.	Perform forensics on cyber events to aid in root cause analysis and residual effects. HSN forensics must accommodate the fact that some of the relevant data may be on a host system or service provider. The forensic team may not have access to all the relevant data.	**CISA-CIVR-PB** [CISA-CIVR-PB] 16 **NIST SP 800-53 Rev. 5** AC-20, IR-4, IR-5, RA-5, SA-9 **NIST SP 800 61 Rev. 2** 3
RS.AN-4: Incidents are categorized consistent with response plans.	Categorize cybersecurity incidents according to the severity and impact consistent with the response plan. Such categorization may include impacts on the hybrid user, community, partners, and third-party stakeholders.	**NIST-SP 800-53 Rev. 5** CP-2, IR-4, IR-5, IR-8, RA-3 **NIST SP 800-61 Rev. 2** 2, 3.2
RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g.,	Establish processes for responding to disclosed vulnerabilities. These processes are especially important when the	**DHS-NCCIC** **GPS-ICD-240** 7.6, 7.7

Respond Analysis		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
internal testing, security bulletins, security researchers).	vulnerability affects the HSN interfaces or data flows.	**NIST SP 800-53 Rev. 5** CA-1, CA-5, CA-7, PM-4, PM-15, RA-1, RA-5, RA-7, SI-5 **NIST SP 800-61 Rev. 2** 3, 3.2 **NIST SP 800-160 Vol. 1 Rev. 1** 3.4.9, 3.4.11

669   ### 4.4.4. Respond: Mitigation Category

670   Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the
671   incident.

672   Mitigation activities will impact partners, stakeholders, and other elements of the HSN.
673   Organizations need to be aware of any undesirable consequences of mitigation measures, and
674   consider the impact on pre-existing MOUs, SLAs, or similar agreements.

675   The Respond improvements category has three subcategories that apply to HSNs.

676   **Table 19.** Mitigation Category for Respond Function.

Respond Improvements		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
RS.MI-1: Incidents are contained.	Contain cybersecurity incidents to minimize impacts on the HSN. Containment may also involve rapidly zeroizing processing equipment that contain sensitive data. Some organizations have remote assets in vulnerable locations, and operators may need to disable equipment quickly. Have processes to enable automated response capabilities to reduce response time for active	**CISA-CIVR-PB** 14 **NIST SP 800-53 Rev. 5** IR-4 **NIST SP 800-61 Rev. 2** 3.4.1

Respond Improvements		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	threats. Consider technologies such as artificial intelligence or machine learning to hasten the response.	
RS.MI-2: Incidents are mitigated.	Once the effects of the incident are contained, take steps to return to a proper working state. These steps should be performed in a manner that does not impact forensic efforts.	**NIST SP800-53 Rev. 5** IR-4 **NIST-SP800-61 Rev. 2** 3.4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	Risk assessments (refer to RA-1) should be updated with newly identified HSN vulnerabilities. Vulnerabilities should be mitigated, or the residual risks documented as acceptable. Revise protection, monitoring, detection, response, and recovery capabilities as needed to mitigate newly identified vulnerabilities in a timely manner.	**NIST SP800-53 Rev. 5** CA-2, CA-7, RA-3, RA-5, RA-7 **NIST SP 800-61 Rev. 2** 3 **RTCA DO-235** 3.8, 14.1.4, 14.2-14.4

4.4.5. Respond: Improvements Category

677

678 Organizational response activities are improved by incorporating lessons learned from current
679 and previous detection/response activities.

680 HSNs will require sharing lessons learned collaboration with partners, service providers and
681 other elements of the HSN. Any changes and improvements will need to be evaluated in the
682 context of their efficacy and impact on the HSN and partners.

683 This category is a post-incident analysis activity involving other CSF functions.

684 The Respond improvements category has two subcategories that are applicable to HSNs.

685　　　　　　　　　　　**Table 20.** Improvements Category for Respond Function.

Respond Improvements		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
RS.IM-1: Response plans incorporate lessons learned.	Share the lessons learned with the participants of the HSN. The elements of the HSN should incorporate the lessons learned into incident response procedures, training, and testing. Keep plans updated and implement the resulting changes accordingly.	**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2**
RS.IM-2: Response strategies are updated.	The response strategies are updated based on the analysis of the event, its corresponding impact to the organization, its impact to the other elements of the HSN and any impacts to the organizations ability to comply with existing MOUs, MOAs or other agreements.	**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8

686　**4.5.　Recover**

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

689　The activities in the Recover Function support timely recovery to normal operations and return
690　the organization back to its proper working state after an incident has occurred. The Recover
691　Function's effectiveness depends on the implementation of the previous Functions: Identify,
692　Protect, Detect, and Respond.

693　The objectives of the recover Function are to:

694　　　• Restore the HSN services to a proper working state using a verified recovery procedure
695　　　　so that systems dependent on those services can function properly.

696　　　• Communicate the recovery activities and status of the HSN services to stakeholders.

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

698 ### 4.5.1. Recovery Planning Category

699 Recovery processes and procedures are executed and maintained to ensure the restoration of
700 systems or assets affected by cybersecurity incidents.

701 In the context of HSN, coordination across the participating organizations in advance of the
702 incident is required to ensure successful recovery. Organizational recovery plans should be
703 coordinated in advance to protect each organization's equities.

704 The Recover recovery planning category has a single subcategory that applies to HSNs.

705 **Table 21.** Recovery Planning Category for the Recover Function.

Recover Recovery Planning		
Subcategory	Applicability to HSNs	References (HSN-Specific)
RC.RP-1: The recovery plan is executed during or after a cybersecurity incident.	The recovery plan can include specific actions for the restoration, recalibration, resetting, and test validation of equipment. Perform system testing to verify the systems are restored to proper working state.	**NIST SP 800-53 Rev. 5** CP-2, CP-9, CP-10, IR-4, IR-8, **NIST SP 800-61 Rev. 2** 3.4

706 ### 4.5.2. Improvements Category

707 Recovery planning and processes are improved by incorporating lessons learned into future
708 activities.

709 In the context of HSN, the efficacy of the recovery actions will require deliberations between the
710 components to capture different perspectives. Proposed improvements are evaluated and agreed
711 upon.

712 The Recover improvements category has two subcategories that apply to HSNs.

713 **Table 22.** Improvements Category for the Recover Function.

Recover Improvements		
Subcategory	Applicability to HSNs	References (HSN-Specific)
RC.IM-1: Recovery plans incorporate lessons learned.	Update the recovery plan to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, the operating environment, and deficiencies encountered	**NIST-SP800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8 **NIST SP 800 612** 3.4

Recover Improvements		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	during plan implementation, execution, and testing.	
RC.IM-2: Recovery strategies are updated.	Evaluate the incident's characteristics and impact to determine if the recovery strategy was sufficient or appropriate (i.e., proportional to the impact) and revise the recovery strategy and corresponding plan accordingly. HSNs share lessons learned and after-action reports among partner organizations in a format and level of detail agreed upon in advance. Consider participation and sharing of lessons learned in forums such as Space ISAC.	**NIST SP 800-53 Rev. 5** IR-3, IR-4, IR-8

4.5.3. Communications Category

Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

In the context of HSN, organizations should compare and communicate post event public relations policies/procedures to plan for after incident response.

The Recover communications category has two subcategories that apply to HSNs.

Table 23. Communications Category for the Recover Function.

Recover Communications		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
RC.CO-1: Public relations are managed.	Coordination among stakeholders needs to occur to ensure a consistent and	**NIST SP800-53 Rev. 5** IR-4, PM-1

Recover Communications		
Subcategory	**Applicability to HSNs**	**References (HSN-Specific)**
	accurate messaging from all the partner organizations.	**ISO/IEC 27001:2022** A.6.1.4, Clause 7.4
RC.CO-2: Reputation is repaired after an incident.	Compare post-event public relations policies/procedures to plan for after-incident response.	**NIST SP800-53 Rev. 5** IR-4 **ISO/IEC 27001:2022** Clause 7.4
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	Communicate recovery activities to all relevant internal and external stakeholders, executive, and management teams. Internal and external stakeholder communications are critical and should be executed in a manner that is consistent with the recovery plan.	**ISO/IEC 27001:2022** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

722 References

723 [3GPP-TR-38-811]   Krause J, Meredith J, Merias P (2017) Study on New Radio (NR) to
724   support non-terrestrial networks, 3GPP Mobile Competence Centre, c/o
725   ETSI 650, route des Lucioles 06921 Sophia Antipolis Cedex, France.
726   https://www.3gpp.org/ftp/Specs/archive/38_series/38.811

727 [CISA-ICS]   Cybersecurity & Infrastructure Security Agency (2020) Securing Industrial
728   Control Systems: A Unified Initiative, Cybersecurity and Infrastructure
729   Security Agency Stop 0380, Department of Homeland Security 245 Murray
730   Lane, Washington, D.C. 20528-0380.
731   https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_C
732   ontrol_Systems_S508C.pdf

733 [CNSSI-4009]   Committee on National Security Systems (2015) *Committee on National
734   Security Systems Glossary*. Committee on National Security Systems
735   Instruction (CNSSI) No. 4009, April 2015. https://rmf.org/wp-
736   content/uploads/2017/10/CNSSI-4009.pdf

737 [DHS-RCF]   Department of Homeland Security (2020) Resilient PNT Conformance
738   Framework. (DHS, Washington, DC).
739   https://www.dhs.gov/sites/default/files/2022-
740   05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf

741 [DIA-SPACE]   Defense Intelligence Agency (2019) *Challenges to Security in Space.*
742   Defense Intelligence Agency, Office of Corporate Communications (OCC),
743   7400 Pentagon, Washington, DC 20301.
744   https://apps.dtic.mil/sti/pdfs/AD1082341.pdf

745 [DHS-NCCIC]   National Cybersecurity & Communications Integration Center (2020)
746   *National Cybersecurity & Communications Integration Center (NCCIC)
747   Overview*. Cybersecurity and Infrastructure Security Agency Stop 0380,
748   Department of Homeland Security 245 Murray Lane, Washington, D.C.
749   20528-0380. https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-
750   2012-MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf

751 [ETSI-TR-101-984] European Telecommunications Standards Institute (2007) *Satellite Earth
752   Stations and Systems (SES); Broadband Satellite Multimedia (BSM);
753   Services and architectures.* (ETSI, 650 Route des Lucioles F-06921 Sophia
754   Antipolis Cedex – France).
755   https://www.etsi.org/deliver/etsi_tr/101900_101999/101984/01.02.01_60/tr
756   _101984v010201p.pdf

757 [IEC-61850-90-4]   International Electrotechnical Commission (2020) Communication
758   networks and systems for power utility automation – Part 90-4: Network
759   engineering guidelines. IEC National Committee of the United States of
760   America, 25 West 43rd Street, 4th Floor, New York, NY.
761   https://webstore.iec.ch/publication/64801

762 [IEC-61850-90-12] International Electrotechnical Commission (2020) Communication
763   networks and systems for power utility automotation – Part 90-12: Wide

764   area network engineering guidelines. IEC National Committee of the
765   United States of America, 25 West 43rd Street, 4th Floor, New York, NY.
766   https://webstore.iec.ch/publication/63706

767   [IETF-RFC-8915]   Dansarie M, Franke D, Sibold D, Sundblad R, Teichel K (2020) Network
768   Time Security for the Network Time Protocol, IETF Administration LLC,
769   1000 N West Street, Suite 1200 Wilmington, DE 19801, USA.
770   https://www.rfc-editor.org/rfc/rfc8915.html

771   [ISO/IEC-27001]   Joint Technical Committee ISO/IEC JTC 1, Information Technology,
772   Subcommittee SC 27, Information security, cybersecurity and privacy
773   protection (2022), Information security, cybersecurity and privacy
774   protection — Information security management systems — Requirements.
775   IEC National Committee of the United States of America, 25 West 43rd
776   Street, 4th Floor, New York, NY. https://www.iso.org/obp/ui/#iso:std:iso-
777   iec:27001:ed-3:v1:en

778   [Li-2020]   Carlson B, Dubovik O, Kahn R, Lacis A, Li J, Li X, Li Z, Nakajima T, Wei
779   J, (2020), Synergy of Satellite and Ground-Based Aerosol Optical Depth
780   Measurements Using an Ensemble Kalman Filter Approach, NASA
781   Goddard Institute for Space Studies, 8800 Greenbelt Rd, Greenbelt, MD
782   20771.
783   https://agupubs.onlinelibrary.wiley.com/doi/epdf/10.1029/2019JD031884

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

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

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

796   [NASIC]   National Air and Space Intelligence Center (2019) *Competing in Space.*
797   (NASIC, Dayton, OH).
798   https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-
799   F%20NV711-0002.PDF

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

804   [NIST-IR-8179]   Bartol N, Boyens J, Paulsen C, Winkler K, (2018) Criticality Analysis
805   Process Model: Prioritizing Systems and Components. (National Institute

806		of Standards and Technology, Gaithersburg, MD), NIST Interagency or
807		Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179
808	[NIST-IR-8270]	Scholl M, Suloway T, (2022) Introduction to Cybersecurity for
809		Commercial Satellite Operations. (National Institute of Standards and
810		Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR)
811		8270. https://doi.org/10.6028/NIST.IR.8270-draft2
812	[NIST-IR-8320]	Banks D, Bartock M, Cherfaoui M, Jordan M, Knoll T, Malhotra A,
813		Pendarakis D, Rao R, Romness P, Savino R, Scarfone K, Shetty U,
814		Souppaya M, Yeluri R (2022) Hardware-Enabled Security: Enabling a
815		Layered Approach to Platform Security for Cloud and Edge Computing
816		Use Cases. (National Institute of Standards and Technology, Gaithersburg,
817		MD), NIST Interagency or Internal Report (IR) 8320.
818		https://doi.org/10.6028/NIST.IR.8320
819	[NIST-IR-8323r1]	Bartock M, Lightman S, McCarthy J, Li-Baboud Y, Brule J, Reczek K,
820		Meldorf K, Northrip D, Scholz A, Suloway T, (2023) Foundational PNT
821		Profile: Applying the Cybersecurity Framework for the Responsible Use of
822		Positioning, Navigation, and Timing (PNT) Services. (National Institute of
823		Standards and Technology, Gaithersburg, MD), NIST Interagency or
824		Internal Report (IR) 8323r1. https://doi.org/10.6028/NIST.IR.8323r1
825	[NIST-IR-8401]	Lightman S, Suloway T, Brule J, (2022) Satellite Ground Segment:
826		Applying the Cybersecurity Framework to Assure Satellite Command and
827		Control. (National Institute of Standards and Technology, Gaithersburg,
828		MD), NIST Interagency or Internal Report (IR) 8401.
829		https://doi.org/10.6028/NIST.IR.8401.
830	[NIST-SP-800-30]	Joint Task Force Transformation Initiative, (2012) Guide for Conducting
831		Risk Assessments. (National Institute of Standards and Technology,
832		Gaithersburg, MD), NIST Special Publication (SP) 800-30.
833		https://doi.org/10.6028/NIST.SP.800-30r1
834	[NIST-SP-800-37]	Joint Task Force, (2018) Risk Management Framework for Information
835		Systems and Organizations: A System Life Cycle Approach for Security
836		and Privacy. (National Institute of Standards and Technology,
837		Gaithersburg, MD), NIST Special Publication (SP) 800-37.
838		https://doi.org/10.6028/NIST.SP.800-37r2
839	[NIST-SP-800-39]	Joint Task Force Transformation Initiative (2011) Managing Information
840		Security Risk: Organization, Mission, and Information System View.
841		(National Institute of Standards and Technology, Gaithersburg, MD), NIST
842		Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39
843	[NIST-SP-800-53]	Joint Task Force, (2020) Security and Privacy Controls for Information
844		Systems and Organizations. (National Institute of Standards and
845		Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53.
846		https://doi.org/10.6028/NIST.SP.800-53r5
847	[NIST-SP-800-61]	Cichonski P, Grance T, Miller T, Scarfone K (2012) Computer Security
848		Incident Handling Guide. (National Institute of Standards and Technology,

849   Gaithersburg, MD), NIST Special Publication (SP) 800-53, Available at
850   https://doi.org/10.6028/NIST.SP.800-61r2

851   [NIST-SP-800-63-3] Grassi P, Garcia M, Fenton J (2017) Digital Identity Guidelines. (National
852   Institute of Standards and Technology, Gaithersburg, MD), NIST Special
853   Publication (SP) 800-63, Rev. 3, Includes updates as of March 2, 2020.
854   https://doi.org/10.6028/NIST.SP.800-63-3

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

859   [NIST-SP-800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh
860   AD, Scholl MA, Stine KM (2011) Information Security Continuous
861   Monitoring (ISCM) for Federal Information Systems and Organizations.
862   (National Institute of Standards and Technology, Gaithersburg, MD), NIST
863   Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-
864   137

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

869   [NIST-SP 800-154] Scarfone K, Souppaya M (2016) Guide to Data-Centric System Threat
870   Modeling. (National Institute of Standards and Technology, Gaithersburg,
871   MD), NIST Special Publication (SP) 800-154.
872   https://csrc.nist.gov/CSRC/media/Publications/sp/800-
873   154/draft/documents/sp800_154_draft.pdf

874   [NIST-SP-800-160v1r1]

875   McEvilley M, Oren J, Ross R (2018) Systems Security Engineering:
876   Considerations for a Multidisciplinary Approach in the Engineering of
877   Trustworthy Secure Systems. (National Institute of Standards and
878   Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-
879   160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

880   [NIST-SP-800-161] Bartol N, Boyens J, Fallon M, Holbrook A, Smith A, Winkler K (2022)
881   Cybersecurity Supply Chain Risk Management Practices for Systems and
882   Organizations. (National Institute of Standards and Technology,
883   Gaithersburg, MD), NIST Special Publication (SP) 800-161 Rev. 1.
884   https://doi.org/10.6028/NIST.SP.800-161r1

885   [NIST-SP-800-175Br1]

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

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

893 [NIST-SP-800-207] Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture.
894   (National Institute of Standards and Technology, Gaithersburg, MD), NIST
895   Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-
896   207

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

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

906 [NIST-SP-1800-34] Boyens J, Diamond T, Grayson N, Paulsen C, W. Polk, Regenscheid A,
907   Souppaya M, Brown C, Deane C, Hurlburt J, Scarfone K (2022) Validating
908   the Integrity of Computing Devices. (National Institute of Standards and
909   Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-34.
910   https://doi.org/10.6028/NIST.SP.1800-34

911 [PPD-21]   Presidential Policy Directive (PPD)-21 (2013) Critical Infrastructure Security
912   and Resilience. (The White House, Washington, DC), DCPD201300092,
913   February 12, 2013. https://obamawhitehouse.archives.gov/the-press-
914   office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-
915   and-resil/

916 [RTCA-DO-235]   Radio Technical Commission for Aeronautics (2008), Assessment of Radio
917   Frequency Interference to the GNSS L1 Frequency Band, 1150 18th NW,
918   Suite 910 Washington, D.C. 20036.
919   https://my.rtca.org/productdetails?id=a1B36000001IckKEAS

920 [USG-FRP]   Department of Defense, Department of Homeland Security, and Department of
921   Transportation (2021) 2021 Federal Radionavigation Plan (Department of
922   Transportation, Washington DC). https://www.navcen.uscg.gov/nav-pubs-and-
923   documents-general-library

924 **Appendix A. List of Acronyms**

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

926 **CSF**
927 Cybersecurity Framework

928 **HSN**
929 Hybrid Satellite Network

930 **IEC**
931 ISO/International Electrotechnical Commission

932 **ISAC**
933 Information Sharing and Analysis Center

934 **ISO**
935 International Organization for Standardization

936 **MOA**
937 Memorandum of Agreement

938 **MOC**
939 Mission Operations Center

940 **MOU**
941 Memorandum of Understanding

942 **NIST**
943 National Institute of Standards and Technology

944 **NIST IR**
945 NIST Interagency Report

946 **PCC**
947 Payload Control Center

948 **PNT**
949 Position Navigation and Timing

950 **RF**
951 Radio Frequency

952 **SLA**
953 Service Level Agreement

954 # Appendix B. Glossary

955 **attack**
956 Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system
957 resources or the information itself. [CNSSI-4009]

958 **availability**
959 Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system
960 resources or the information itself. [CNSSI-4009]

961 **bus**
962 The primary spacecraft structure containing power, temperature control, and directional thrusters of the satellite that
963 provides locations for the payloads. [NASA-smallsat]

964 **component**
965 A hardware, software, or firmware part or element of a larger system with well-defined inputs and outputs and a
966 specific function. [DHS-RCF, Adapted]

967 **confidentiality**
968 Preserving authorized restrictions on information access and disclosure, including means for protecting personal
969 privacy and proprietary information. [NIST-FIPS-200]

970 **hybrid satellite networks**
971 An integrated terrestrial and space infrastructure comprised of independently owned and operated segments, parts,
972 or systems that collectively create or perform as a singular space system.

973 **integrity**
974 A measure of the trust that can be placed in the correctness of the information supplied by an HSN service provider.
975 Integrity includes the ability of the system to provide timely warnings to users when the HSN data should not be
976 used. [USG-FRP]

977 **payload**
978 Elements of the spacecraft that provide (commercial, scientific, or other) services to end-users. [NASA-smallsat,
979 Adapted]

980 **payload control center**
981 A facility that provides C2 for satellite payloads.

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

986 **risk**
987 A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a
988 function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of
989 occurrence. [NIST-SP-800-37]

990 **risk assessment**
991 The process of identifying, estimating, and prioritizing risks to organizational operations (including mission,
992 functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from
993 the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and
994 considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST-SP-
995 800-30]

996 **risk management**
997 The program and supporting processes to manage information security risk to organizational operations (including
998 mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation and

999   includes (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once
1000 determined, and (iv) monitoring risk over time. [NIST-SP-800-39]

Risk Management Framework

1001
1002 The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured
1003 process that integrates information security and risk management activities into the system development life cycle.
1004 [NIST-SP-800-37]

secure

1005
1006 To reduce the risks of intrusions and attacks as well as the effects of natural or manmade disasters on critical
1007 infrastructure by physical means or defensive cyber measures. [PPD-21]

threat

1008
1009 Any circumstance or event with the potential to adversely impact organizational operations, organizational assets,
1010 individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure,
1011 modification of information, or denial of service. [NIST-SP-800-53]

verification

1012
1013 Process of producing objective evidence that sufficiently demonstrates that the system satisfies its security
1014 requirements and security characteristics with the level of assurance that applies to the system. [NIST-SP-800-
1015 160v1r1 (§3.4.9), adapted]

vulnerability

1016
1017 A weakness in an information system, system security procedures, internal controls, or implementation that could be
1018 exploited or triggered by a threat source. [NIST-SP-800-30]