NIST Technical Note
NIST TN 2272

Application of the Hybrid Satellite Network Cybersecurity Framework Profile

An Example Implementation of NIST IR 8441

Frederick Byers
Dan Mamula
Karri Meldorf
Joseph Brule
Rory Jennings
John Wiltberger
Eugene Craft
John Dombrowski
O'Ryan Lattin
Abdul Noor
Matt Yetto
Aliaksander Mamonau
Oksana Slivina
Jay Sharma
Kangmin Zheng

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2272

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

NIST Technical Note
NIST TN 2272

Application of the Hybrid Satellite Network Cybersecurity Framework Profile

An Example Implementation of NIST IR 8441

Frederick Byers
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Dan Mamula
Karri Meldorf
Joseph Brule
Rory Jennings
John Wiltberger
Eugene Craft
John Dombrowski
O'Ryan Lattin
Abdul Noor
Matt Yetto
Aliaksander Mamonau
Oksana Slivina
Jay Sharma
Kangmin Zheng
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2272

February 2024

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

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

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

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-01-30

How to Cite this NIST Technical Series Publication:
Byers F, Mamula D, Meldorf K, Brule J, Jennings R, Wiltberger J, Craft E, Dombrowski J, Lattin O, Noor A, Yetto M, Mamonau A, Slivina O, Sharma J, Zheng K (2024) Application of the Hybrid Satellite Network Cybersecurity Framework Profile: An Example Implementation of NIST IR 8441. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) NIST TN 2272. https://doi.org/10.6028/NIST.TN.2272

Author ORCID iDs
Frederick Byers: 0009-0005-7865-2628
Dan Mamula: 0000-0003-4247-1735
Karri Meldorf: 0000-0003-3617-3846
Joseph Brule: 0000-0002-7987-6050
Rory Jennings: 0000-0001-5860-5094
John Wiltberger: 0000-0002-6412-8105
Eugene Craft: 0009-0009-0164-1241
John Dombrowski: 0000-0002-9408-1838
O’Ryan Lattin: 0000-0003-4255-280X
Abdul Noor: 0009-0002-8716-5731
Matt Yetto: 0009-0007-6913-1227
Aliaksander Mamonau: 0009-0005-0358-3357
Oksana Slivina: 0009-0006-6857-9778
Jay Sharma: 0000-0002-0876-7973
Dr. Kangmin Zheng: 0009-0008-0857-5921

Contact Information
hsn_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002

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

Abstract

The space sector is transitioning towards Hybrid Satellite Networks (HSN), 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 cybersecurity framework is required to assess the security posture of the individual components while still enabling the HSN to provide its function. NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks, applies the NIST Cybersecurity Framework Version 1.1 to address cybersecurity risks specific to HSN. This technical note presents a fictitious organization with common scenarios they are likely to encounter with their hosted payload. Results of the lab tested examples are presented to provide further context for an organizational application of the HSN profile.

Keywords

Cybersecurity Framework; hosted payload; HSN; Hybrid Satellite Networks; profile; risk management; security assessments.

Note to Readers

This document is an example implementation of NIST IR 8441, Cybersecurity Framework Profile (CSF) for Hybrid Satellite Networks, that provides voluntary guidance and does not issue regulations, define mandatory practices, provide a checklist for compliance, nor does it carry statutory authority. It is intended to be a foundational set of guidelines.

Additionally, the full analysis for all 104 CSF subcategories is presented in Appendix A.

Table of Contents

List of Tables

List of Figures

1. Introduction

A Hybrid Satellite Network (HSN) uses independently owned and operated terrestrial and space components to realize a space system. The HSN architecture typically consists of a combination of independently owned terminals, antennas, satellites, payloads, or other components that communicate across disparate networks. An HSN may interact with government systems and critical infrastructure (as defined by the Department of Homeland Security) to provide services such as satellite-based communications, position, navigation, and timing (PNT), remote sensing, weather monitoring, and imaging. An HSN is likely to have varying levels of trust among different components, requiring frameworks for establishing confidentiality and integrity of individual elements while still enabling availability of required shared services.

The purpose of this paper is to provide an example implementation of how to use the NIST IR 8441 Cybersecurity Framework (CSF) Profile for Hybrid Satellite Networks. This includes likely threat scenarios an HSN organization may face for their hosted payload plus a description of how a fictitious HSN organization applies the HSN CSF profile. This paper also presents the results of tests that were performed in a real lab, the Commercial Cyber Resilience Lab. Organizational profiles are specific to individual scenarios and missions, and as such, the assumptions, findings, or assessments for scenarios presented in this paper should not be assumed to be relevant to another scenario.

2. Background

This section presents important background information describing the NIST Cybersecurity Framework 1.1 and its purpose with relation to NIST IR 8441 and this technical note. Also presented in this section is a summary of NIST IR 8441 and the likely organizational roles and their responsibilities within an organization that have equity in hosted payload security.

2.1. NIST Cybersecurity Framework (CSF) 1.1

The purpose of the NIST CSF is to provide a means for an organization to reduce cybersecurity risks by understanding, assessing and communicating its cybersecurity posture using a common language and systematic methodology. An organization can use the CSF to guide a review of the state of their operation from the perspective of five high-level Functions, Identify, Protect, Detect, Respond, and Recover. Analysis of that operational review allows an organization to draft an current state or a target state CSF Profile. Organizations can also use the CSF to support their current risk management processes.

2.2. Purpose of the CSF and CSF Profile NIST IR 8441

The CSF provides guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risks. In addition to helping organizations manage and reduce risks, it is designed to foster risk and cybersecurity management communications amongst internal and external organizational stakeholders.

A sector-specific or community CSF profile focuses on how a particular CSF Category or Subcategory applies to sector or community's generalized cyber-ecosystem. NIST IR 8441 serves as a sector-specific or community profile for how organizations can apply the NIST CSF. It is intended to be a starting point when analyzing a specific activity, project, business, or organization. Given that organizations will have their own goals, priorities, risk tolerance, and definition of what assets are critical, then it follows that NIST IR 8441 cannot proscribe specific implementations, define a set of tasks, or recommend specific measures. Thus, organizations will need to tailor and augment the information in NIST IR 8441 to meet their organization-specific needs by creating an organizational CSF profile. An organizational CSF profile is created by implementating the CSF profile. This document provides an example of creating an organizational CSF profile and also provides test results from three (3) likely cyber security incident examples to add additional context for the benefits of creating an organizational CSF profile. For the scenario provided in this paper, an organizational profile (NIST TN 2272) is created based on the community profile CSF HSN Profile (NIST IR 8441). In this document we analyze each CSF subcategory as shown in Appendix A, but only a subset were analyzed for the operational examples.

2.3. NIST IR 8441 Summary

NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) describes how an organization may assess the cybersecurity posture of their HSN. NIST IR 8441 presents the CSF subcategories in the context of the HSN cyber-ecosystem and provides a useful list of informative references relevant to the sector to aid stakeholders when applying the CSF to their organization.

A CSF profile can be used for different purposes and be applied at different stages in the lifecycle of a satellite system. In this document, the profile will be applied at the operational phase to show how the CSF can be used to communicate the organization's security posture so that informed risk management decisions can be made. However, NIST IR 8441 may be integrated at any system lifecycle stage and can be applied iteratively for cybersecurity assessments and improvement measurements.

HSN organizations may implement an organizational CSF profile by customizing the HSN sector-specific CSF profile from NIST IR 8441 for their specific organization. When completed, an organizational CSF profile provides the stakeholder a customized snapshot of their "as is" or target ("to be") cybersecurity posture.

2.4. CSF Organizational Roles and Responsibilities

As mentioned in section 2.3, organizational profiles are developed to an organization's specific needs and will require participation by several people within the organization. Creating an organization CSF profile could also include participation from third-party partners, customers, or other stakeholders. Organizations have different assets, architectures, cybersecurity resources, and tolerances to a loss of assurance. A systematic assessment of the cybersecurity posture requires knowledge of assets, any cybersecurity measures in place, knowledge of any external dependencies, and the impact to the organization should a threat be realized. Generating the assessment and definition of a way forward to achieve the appropriate level assurance will require stakeholders to include, leadership and a cadre of subject matter expertise such as:

- The Chief Information Officer (CIO). Manages people, processes, and technologies within the organization with the ability to influence the direction of resources for greater assurance or accept the residual risk.
- Cybersecurity Experts. Provide knowledge of cyber-threats and the ability of the current or proposed HSN's ability to mitigate attacks.
- Operators and Operations Management. Provides knowledge of daily operations and the impact of an incident.
- Users of HSN-Generated or Provided Data. Provide insight on the impact should the organization's products or services be delayed, degraded, or lost.
- System Administration. Configures systems or gathers information to provide data for engineering, analysis or enforce technical and managerial controls.
- IT and System Design. Provides knowledge of current or proposed designs and may propose new or modified components or systems.
- System Engineering. Integrates modifications or designs of the HSN.

- Marketing, Sales, and Business. Provides insight regarding how an incident would impact marketability, future sales, and reputation of the organization.

Once the stakeholder team is assembled and the background information is made available, a systematic assessment of subcategories can be made in the context of the individual organization. The findings of the stakeholder team will enable executives and leaders to make informed decisions regarding the “as is” or target (“to be”) posture.

3. Hosted Payload Scenario

In order to provide a reference example, a fictitious organization was created to represent a HSN. An overview of the mission objectives, operations/business model, and description of the HSN are discussed to provide context for the reference example. It is assumed the fictitious organization has accomplished the overview prior to implementation of the HSN CSF Profile (NIST IR 8441). For this paper, the fictitious organization is called SaveForests and it uses an HSN for a camera hosted payload to meet its mission objectives. A hosted payload is an easy example of an HSN that can be used to illustrate the process of developing the custom profile. A systematic assessment of NIST IR 8441 in the context of the SaveForests organization is presented in Appendix A and Sec. 3.2.1 will highlight some of the threats and impacts from the assessment.

3.1. SaveForests Foundation

The SaveForests Foundation is a not-for-profit organization whose mission is to monitor and call attention to the health of the world's forests. As a part of its mission, SaveForests requires overhead optical data to monitor the progression of events such as forest fires and perform spectral analysis to assess changes in the health or diversity of forests throughout the world.

3.1.1. Mission Objectives

SaveForests has the following mission objectives:

- To assess and protect the health of the world's forests based on the analysis of overhead imagery data that are regularly updated.
- To provide analysis of data to stakeholders such as foresters, environmentalists, governments, and academics to answer questions such as the progression of disease, habitat loss, impact of catastrophic events, and success of reclamation efforts.
- To become a trusted source of accurate and precise data and information related to forests.

3.1.2. Operations and Business Model

To achieve these objectives, SaveForests will have a team of data scientists and biologists who will apply algorithms and analytic tools to optical imagery collected over time that will provide insight into the nutritional health, disease progression and other impacts to the forest ecosystem.

SaveForests' reputation as a source of accurate analysis is paramount; therefore, the images to be analyzed will be collected from a space-based camera that is owned and operated by SaveForests to assure the authenticity and integrity of the raw data and the subsequent analysis.

Though SaveForests' primary mission is to provide trusted analysis of the health of the forests, the company may provide imagery services to other organizations that require or can benefit from SaveForests' ability to provide photography of earth objects in near real time on a 24/7 basis with a daily revisit in daylight conditions.

As a part of its operations, SaveForests requires overhead optical data to monitor the progression of events such as forest fires and perform spectral analysis to assess changes in the health or diversity of forests throughout the world. SaveForests determined that optical cameras in low earth orbit (LEO) will provide global coverage and will revisit a general area each day.

3.1.3. SaveForests HSN

Space operations are resource intensive and SaveForests wants to focus its resources on its primary mission, performing analytics. The camera itself was acquired from the camera vendor Payloads-R-Us company. SaveForests will be in full control of the day-to-day operations of the payload and has contracted with Payloads-R-Us to maintain the payload for the entire life of the host satellite.

SaveForests contracted with SatCo to host the camera payload on a low earth orbit (LEO) commercial satellite. SaveForests will control the payload from its headquarters. SatCo will forward commands from SaveForests to the payload, receive transmissions from the payload, and forward the payload data to the SaveForests headquarters.

The SatCo satellite provides all the communication networks, interfaces, and power to make the camera system function. SatCo has contracts with the company GroundSyn to provide global communication services to SatCo satellites. The camera is controlled from SaveForests' payload control center (PCC) that is at a different location than SatCo's satellite mission operations center (MOC).

As depicted in Fig. 1 below, the SatCo satellite has its own operational payload (Payload A), a hosted payload from a different corporate entity (Payload C), and the SaveForests hosted camera payload (Payload B). Each payload communicates with the satellite through a common spacecraft bus interface. SatCo's satellite is operated in the LEO and is connected through radio frequency (RF) transmissions for satellite operations and transfer of mission data. The MOC will ingest all data from the hosted payloads and forward the data to the respective payload owners. Spacecraft data will be received by the ground station as a service provider GroundSyn. There will be multiple ground reception stations throughout the world, and that data will be transmitted to the MOC via terrestrial links.

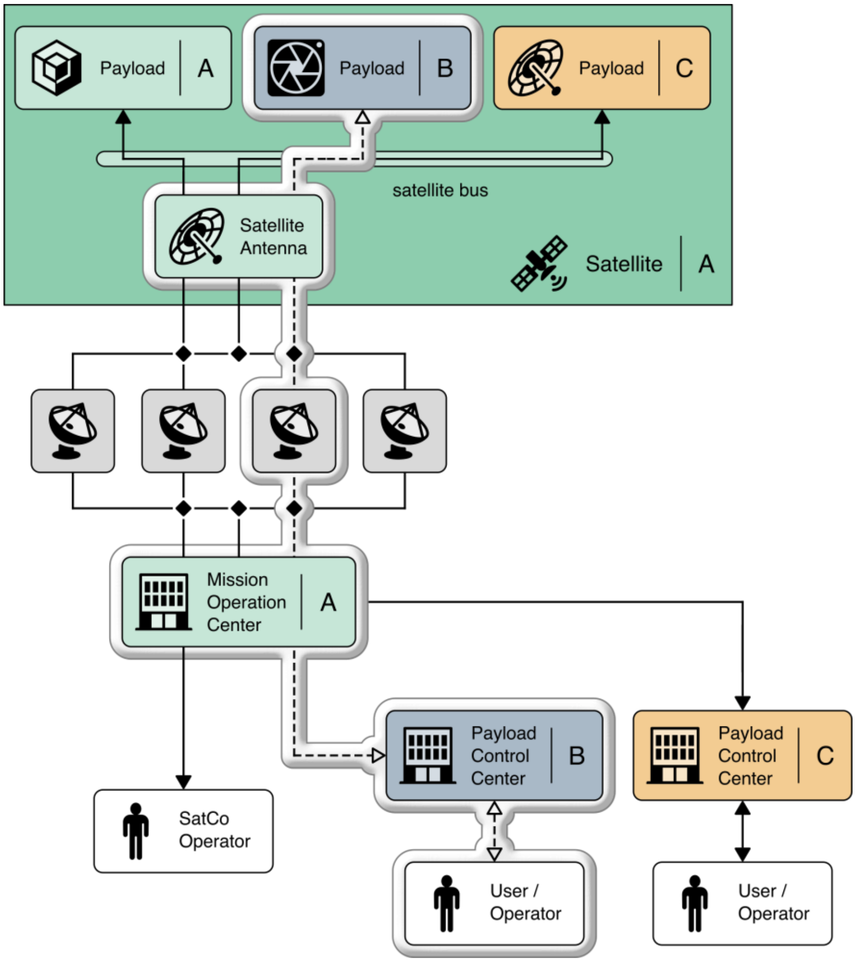

Fig. 1. SatCo Satellite System Overview.

3.2. Application of the CSF Profile: Current Cybersecurity Posture

The cybersecurity of SaveForests' HSN is impacted by its assets (payload, PCC systems, and associated software), its supply chain, agreements and contracts with external organizations including Payloads-R-Us, and SatCo for hosting the payload and associated SatCo systems and software (MOC, satellite, communication systems). The HSN may be affected by SatCo's partners and service providers such as GroundSyn and the owner of Payload C.

SaveForests assessed their current cybersecurity posture by using NIST IR 8441 as the starting point from which to create their organization-specific profile. Analysis of the current cybersecurity posture led to a list of threats and impacts to their business and a decision to test implementations of additional cybersecurity measures in a lab.

3.2.1. Assessment: SaveForests' Current Cybersecurity Posture

The Chief Information Officer at SaveForests assembled a team of experts including cybersecurity experts, satellite experts, SaveForests analysts, and the head of the business development and marketing team. This team performed a systematic analysis of its cybersecurity posture by using the subcategories identified in NIST IR 8441 as most relevant to HSN. NIST IR 8441 presents 104 subcategories from the CSF that are applicable to HSNs for consideration and the assembled stakeholder team evaluated each of these in the context of the SaveForests cyber-ecosystem.

The tables below illustrate examples of “not applicable” for three of the NIST IR 8441 subcategories for the SaveForests HSN. The team concluded that some parts of these subcategories are not applicable in the context of the SaveForests organization. In Table 1, SaveForests imagery collections are in remote forested areas and do not involve occupied structures or populated areas, therefore, concerns regarding privacy and civil liberties noted in the CSF ID.GV-3 subcategory do not apply. In Table 2, SaveForests’ mission neither directly supports nor is part of the supply chain or critical infrastructure noted, respectively, in the CSF ID.BE-1 and ID.BE-2 subcategories.

A full review and analysis of the entire list of 104 subcategories should be accomplished during a CSF Profile implementation. For reference, Appendix A presents an analysis for all 104 subcategories for the SaveForests HSN.

Table 1. Governance Category for the Identity Function ID.GV.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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).	**Payload owner Organization:** SaveForests should review legal and regulatory requirements, however, their primary mission involves the monitoring and assessment of the health of forests and is not likely to include civil liberties or privacy issues.
		Partner Organizations: SatCo: SatCo provides bent pipe transponders for hosted payloads, and it is the responsibility of the mission and data owners to address issues associated with civil liberties and privacy issues.

Table 2. Business Environment Category for the Identity Function ID.BE.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.BE-1: The organization's role in the supply chain is identified and communicated.	Identify the role in the supply chain and consider any partners' role in the supply chain. Clearly communicate any corresponding expectations and requirements.	**Payload owner Organization:** SaveForests does not actively perform supply chain aspects of CSF and contracted for those services with Payloads-R-Us for the payload. **Partner Organizations:** SatCo and Payloads-R-Us role in the supply chain is defined in contractual documents.
ID.BE-2: The organization's place in critical infrastructure, and its industry sector is identified and communicated.	Placement in critical infrastructure is based on the service(s) provided (such as Communication services, Emergency services and others). 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 corresponding expectations. Capture the partner's requirements in addition to what will be provided to fulfill the operational objectives.	**Payload owner Organization:** SaveForests is not a part of the critical infrastructure. **Partner Organizations:** The mission is not part of the critical infrastructure.

It is important to highlight that there will not always be a fully informative assessment of a subcategory. Sometimes a CSF subcategory cannot be fully assessed due to a lack of information, for example, lack of information about the other payloads hosted by SatCo.

Table 3 discusses the likelihood of how an attack affects the SaveForest capability and intent of a potential adversary; however, SaveForests does not have detailed information about the other payloads on SatCo, hence, is unable to assess a potential adversary's intent to attack the satellite's mission downlink.

Table 3. Risk Assessment Category for the Identity Function ID.RA.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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), Memorandum of Understanding (MOU), Service Level Agreement (SLA) or similar document.	**Payload owner Organization:** A loss of availability of the mission downlink results in a loss of some data points which degrades subsequent analysis but does not lead to mission failure or high loss. The intent for an adversary to deny the downlink to SaveForests is low, however, a downlink jamming attack intended for another mission would also deny SaveForests. The intent for an adversary to deny the downlink to other payload owners is unknown. The likelihood of a successful availability attack or the inability to receive the mission downlink is indeterminant.

The team was able to assess how well specific CSF sub-categories were addressed with varying levels of precision. For example, in Table 4 and Table 5, SaveForests' participation in information sharing forums was found to be inadequate due to the organizations' limited resources; conversely, the strength of authentication was well documented and shown to be robust.

Table 4. Risk Assessment Category for the Identity Function ID.RA.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources	Consider joining an organization or forum such as the Space Information Sharing and Analysis Center (ISAC).	**Payload owner Organization:** SaveForests is a small organization whose expertise is in biology and has limited resources. SaveForests does not actively search out or directly receive cyber threat intelligence during normal operation. **Partner Organizations:** SatCo: SatCo receives cyber threat intelligence as part of its normal operations through manual research and cloud-based intelligence feeds in its ground-based cyber systems.

Table 5. Access Control Category for the Protect Function PR.AC.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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).	Consider 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 may be a priority. Evaluate the risks and implement adequate controls in accordance with the diversity of the HSN. Consider controls such as multi-factor authentication.	**Payload owner Organization:** Interactions with the SaveForests database requires an Short Message/Messaging Service (SMS) verification in addition to a username and password. **Partner Organizations:** SatCo: The MOC at SatCo required the use of a token associated with a particular computer in addition to a username and password.

The analysis also showed where CSF subcategories were sufficiently addressed albeit indirectly. For example, in Table 6, SaveForests does not have satellite expertise but satisfactorily addressed issues through MOAs or SLAs.

Table 6. Information Protection Processes and Procedures Category for the Protect Function PR.IP.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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 can be applicable.	**Payload owner Organization:** SaveForests' vulnerability management plan for the payload is coordinated with SatCo and is supported by the payload vendor. SaveForests" vulnerability plan for non-payload/satellite specific considerations are already implemented and follows industry best practices. SaveForests relies on the automatic update functions provided by Cost of the Shelf (COTS) products for software and Internet Technology (IT) **Partner Organizations:** SatCo: SatCo coordinates payload vulnerability management plans with SaveForests and each payload owner.

3.2.2. Threats and Impacts

The threats and corresponding impact of concern to SaveForests are comprised of the following:

- A loss of its ability to collect new data: SaveForests needs to regularly collect imagery to validate its previous projections, update its analysis and provide new analysis for the stakeholder community. The inability to collect future imagery would be catastrophic. (ID.BE-3, ID.BE-4, PR.DS-4)
- A loss of archived data: SaveForests' mission is to provide analysis and projections. Should the archived data be lost, SaveForests will be unable to fulfill its primary mission, and, hence, a loss of archived data is catastrophic. (ID.BE-3, ID.BE-4, PR.DS-1, PR.DS-4)
- A loss or degradation of data integrity: One of SaveForests' greatest assets is its reputation as a trusted and accurate source of information. A degradation in the integrity of the data and information will result in a corresponding reduction in the confidence and trust that the stakeholders have in SaveForests. (ID.BE-3, PR.DS-1, PR.DS-2, PR.DS-4)
- An interruption in the availability of new imagery data: SaveForests performs trend analysis and projections for its stakeholders. A disruption in the flow of new imagery data leads to a corresponding degradation in the precision of the trend analysis and projections. The impact should this threat be realized is proportional to the duration of the outage. (ID.BE-3, ID.BE-4, PR.AC-5, PR.DS-4)
- A loss of integrity in the imagery feeds: Should the accuracy and precision of the imagery feeds be compromised, then the subsequent analysis will be degraded, and if the duration and scope integrity compromise remain unknown, then the integrity and subsequent analysis of the archived data will be called into question. The impact of a loss of integrity to a constrained set of data is proportional to the amount of data in question. A loss of integrity that leads to a lack of confidence in the entire data set is catastrophic. (ID.BE-3, PR.AC-5, PR.DS-2)
- A loss of confidentiality in the imagery feeds. SaveForests may task the camera to collect raw imagery to other organizations that may be sensitive to the other party. Should the confidentiality of the feed be compromised, then future clients will be less likely to purchase imagery feeds. The impact to future business due to a loss of confidentiality is severe. (ID.BE-3, PR.AC-5, PR.DS-2, PR.DS-5)

Based on an analysis of threats to space systems and cyber threats to information systems, the following attacks, their corresponding impact, and the likelihood of the realization of the threat that are applicable to the HSN as implemented by SaveForests were identified:

- Physical destruction of the host would end SaveForests' ability to collect future imagery. The realization of this attack will cause SaveForests to fail due to the cost of replacing the on-orbit camera in a timely manner and the lack of new data for future analysis. Though the likelihood of physical destruction is very low, the impact is critical. SaveForests has chosen to transfer the risk and purchased an insurance policy to replace the payload in the event of physical destruction. (refer to subcategories ID.RA-1, ID.RM-4)

- A payload command link intrusion would interrupt SaveForests' ability to obtain new imagery: An adversary formats a command in a frame that is compatible with SatCo's bus and transmits the command to the satellite, which will cause the camera to change its pointing angle. The impact of a payload command link intrusion is moderate due to the irrecoverable loss of data points, but the likelihood of a command link intrusion is very low because SatCo encrypts the command uplinks, and the satellite will ignore any plaintext commands from the ground. SaveForests has chosen to accept the risk of an RF-based command link intrusion. (refer to subcategories ID.RA-1, ID.RM-4, IP.DS-3)
- A downlink jammer directed at the GroundSyn station leased by SatCo: An adversary deploys a downlink jammer near the GroundSyn antenna. The jammer has two modes, a periodic pulse that introduces errors and leads to corrupted frames and a higher-powered continuous signal that leads to a loss of the satellite signal. The impact of a downlink jammer is moderate due to the irrecoverable loss of data points. The likelihood of a downlink jamming attack is indeterminate. A potential adversary's motivation to deny SaveForests data is low. However, downlink jamming is relatively simple and an attacker targeting a different payload will also deny SaveForests' mission data. The likelihood of attacking the other payloads is unknown. SaveForests has chosen to accept the risk with the understanding that this is a lower priority.
- A downlink RF transmitter that spoofs the satellite mission data downlink. The adversary generates a signal that is compatible with the waveform but populated with false data. The impact of downlink spoofing is moderate (irrecoverable loss of data points) to high (a loss of integrity that calls to question the validity of SaveForests' analysis). The likelihood of downlink spoofing is low due to the technical difficulty of inserting false data that would not be detected. SaveForests has chosen to accept the risk.
- A passive RF collection device is deployed within the downlink beam. The adversary can collect and use the mission data for their own purposes. The likelihood of this attack is very high due to the widespread availability of RF receivers and the number of potential attackers. Initially SaveForests assessed the impact to be low because SaveForests' mission is to disseminate the health of the forests and open to independent analysis; however, the head of the marketing department raised a concern that some of the SaveForests' clients may consider data that SaveForests collects on their behalf to be sensitive. SaveForests has chosen to mitigate the risk due to the impact on future clients.
- A backdoor intended for the payload that is implanted within a deployed software patch. This backdoor can cause the disruption of image capture resulting in a loss of data points to support SaveForests' analysis. The likelihood of this backdoor is medium. SaveForests has chosen to mitigate this attack by security controls and the implementation of payload script signals to detect discrepancies between the deployed files and the gold standard files.

- A separate payload hosted on the SatCo bus captures SaveForests' data on the bus and can send commands to the SaveForests' payloads (bypassing the MOC). The software connection from SatCo's satellite bus to the payloads are through the Controller Area Network (CAN bus) and Serial Peripheral Interface (SPI). A CAN bus is a lightweight protocol that does not have built in authentication measures. From a technical point of view, this attack is quite feasible, and an adversary could infiltrate another organization's capability to gain access to partner organizations. The likelihood of this attack is medium. The impact to SaveForests ranges from a temporary loss of imagery data points to a loss of control of the payload. SaveForests has chosen to mitigate this attack by encrypting communications so that only company assets can see images and communicate with the payload. (refer to subcategories ID.AM-2, ID.RA-1, ID.RA-5)

3.3. Application of the CSF: Analysis of Mitigation Measures

Based on the current cybersecurity posture of SaveForests, the Chief Information Officer has chosen to apply cybersecurity measures to mitigate risks that are identified in the key findings. To verify that the cybersecurity measures are at the desired level of security, SaveForests will execute a series of tests on a test and evaluation (T&E) payload in its lab. The lab is necessary because, once the satellite is launched, cyber security measures will be difficult to test and incorporate. The lab will be used for purpose of describing the test environment and executing the tests.

3.3.1. Description of Lab Environment

An actual lab was used for testing and results to illustrate how the profile can be applied. The Commercial Space Cybersecurity Resilience Lab (CSCRL) has the purpose of testing the efficacy of cybersecurity measures to mitigate attacks on commercial satellites. The CSCRL facilitates research of commercial satellite operator ideas, recommendations, and potential solutions to help reduce vulnerabilities within and around their satellites. It consists of an actual 3-Unit (3U) CubeSat and includes modeled ground segment systems and components that interface with the space vehicle and its payload.

The goal of this CSCRL is to produce open, standards-based, adaptable recommendations that address the security challenges faced by small commercial satellite operators to aid them in improving their overall cybersecurity posture. The work conducted in the CSCRL will examine how a malicious actor could compromise a satellite and what impact they could have. The output will be recommendations geared towards helping commercial satellite operators implement stronger cybersecurity practices and programs.

3.3.2. Lab Architecture

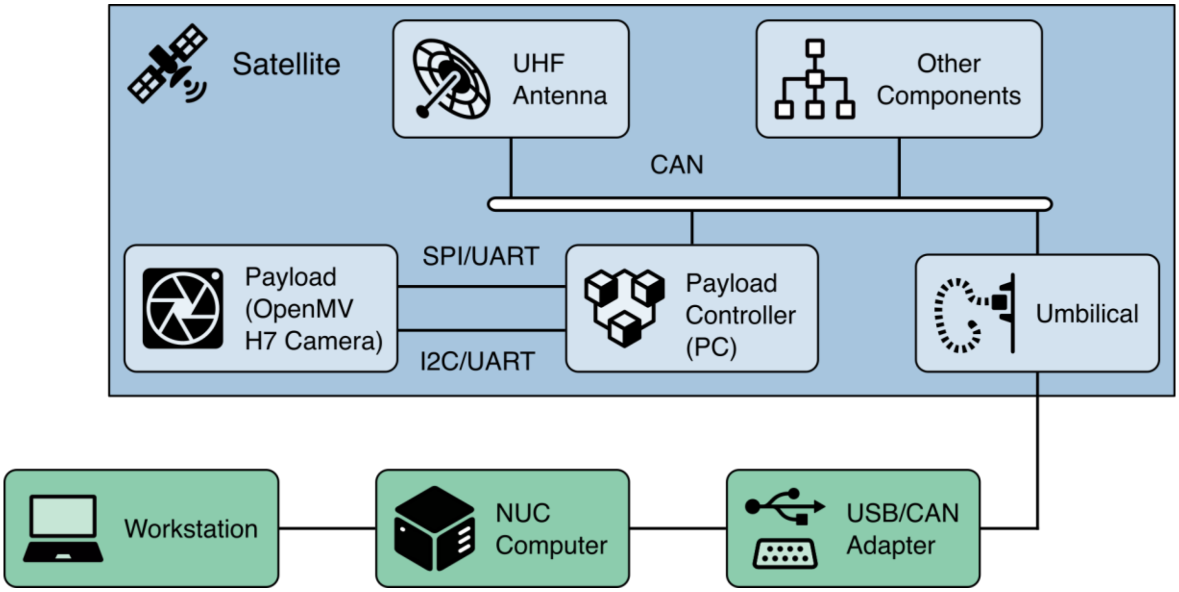

Fig. 2. Commercial Space Cyber Resilience Lab (CSCRL).

Figure 2 above illustrates the lab architecture. The ground segment consists of a Next Unit of Computing (NUC) computer, a Controller Area Network (CAN) adapter, and an umbilical board that connects the ground station to the satellite and enables remote access to the CubeSat. The ground control of the satellite is achieved by using the control software application supplied by the satellite vendor. The NUC computer is networked to allow operators/testers/engineers to access the ground control station remotely for testing and configuration of the satellite.

The CSCRL Link Segment capability for communicating with the satellite is “modeled” via a Universal Serial Bus (USB) link.

On the NUC ground station machine, satellite commands and controls will be sent to the satellite from a user-friendly locally hosted web application. This application currently has functions developed for the payload controller system that allow for images to be captured, transferred, and viewed from the onboard payload camera. The web application is designed to provide future support for the different subsystems of the satellite. The setup allows any user accessing the NUC computer directly or remotely to access the web application page.

The CSCRL will be used to show how a hosted payload, in this case the camera, can be secured by using the guidance of the HSN Cybersecurity Profile. The CSCRL will show examples of how the profile can be implemented with the lab results.

The CSCRL emulates RF transmissions by using an umbilical cable to the satellite. The communications between the satellite bus and the payload are at the data link layer (layer 2) that is independent of how the satellite sends to, or receives data from, the ground site. The emulation of RF transmissions does not impact the testing of the payload.

4. Operational Examples

Operational examples of relevant real-world cyber capabilities were developed to help show the reader how to implement the HSN profile. The chosen examples show how some capabilities can be demonstrated and tested.
The sections below detail test-based operational examples that were conducted in the lab environment. These examples highlight examples of how an organization would test implementations to address issues that were identified by their cybersecurity assessment. In this scenario, SaveForests used NIST IR 8441 as its baseline. Three sets of tests were conducted to demonstrate how an implementation would address issues identified during subcategory evaluations. For a detailed description of test procedures for each of these operational examples, see Appendix B: Scenario Implementation Evaluation.

4.1. Hosted Payload Fault (Test Use Summary and Test Objective)

Test Use Summary: The camera is currently in use aboard a satellite and develops a situation that results in a fault code during operation. This fault may be caused by the camera itself or a cyber intrusion. The fault is then transmitted through the payload controller of the SatCo satellite to the ground system. The fault is then analyzed to determine what has happened and how it can be resolved.

Further analysis will be used to determine whether a cyber event has occurred.

Test Objective: Verify capability to detect faults inside of data from payload.

Operational Process:

- Detection of fault code.
- Fault code is transmitted to the ground station for analysis.
- Fault code is analyzed using camera data.
- Camera is inspected and goes through hardware and software diagnostics.
- Procedures and actions to return to normal service.

4.1.1. Details

A hosted payload fault may occur for various hardware, software, and external reasons.

Some examples of the camera malfunction may include:

- Camera shows an error message when it cannot recognize the memory card.
- Memory card have no space to store additional pictures or camera shows a read-only error.
- A battery/power problem causes the camera to not get enough power from the satellite.
- Dust or dirt deposits on lenses due to tiny particles of solid material floating in low orbit (cosmic dust) can cause a lens error.

- Physical environment aspects, including a loss of power, communication interference, etc.
- Additional payloads hosted on the SatCo satellite may affect the health of the SaveForests' payload.

4.1.2. Related CSF Subcategories.

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

The fault detection implementation being tested will monitor the following events that are documented in the SaveForests' baseline of the expected data flow and network operations:

1. Commands from the Payload Control Center, through the Mission Operation Center and SatCo satellite to the payload.
2. Images from the payload through the SatCo satellite and Mission Operation Center to the Payload Control Center.
3. Communications between the payload and SatCo satellite.
4. Communications between the Payload Control Center and Mission Operation Center.

DE.AE-2: Detected events are analyzed to understand attack targets and methods

SaveForests uses commercial off-the-shelf software communication tools to handle, decompress, and translate the raw data from the payload. SaveForests also contracts with the payload vendor to analyze the raw telemetry from the payload to detect and analyze on-orbit attack targets and methods.

The fault detection implementation being considered will be tested to demonstrate that it performs the following tasks:

- Payload faults are analyzed to find the root cause.
- The ground station operator has the capabilities to initiate payload hardware and software diagnostics.

DE.DP-4: Event detection information is communicated.

The fault detection implementation being considered will be tested to demonstrate that it performs the following tasks:

- Automatically transmit a payload fault code that deviates from the baseline to the ground station operator in near real time.
- Diagnostic and camera data shall be sent to the ground station for analysis within a predetermined time.

4.2. Hosted Payload File Modification

Test use summary: A hosted payload file can be tampered with or corrupted incidentally or due to a cybersecurity attack. When a modified picture file is returned from the camera to the ground station, this should trigger alerts. Verifying the integrity of the camera application software files to determine if tampering has occurred by comparing them to a trusted code will protect hosted payload files from unauthorized changes.

Test Objective: Verify capability to determine data integrity from payload.

Operational Process:

- The external security device's hash detection script is triggered either prior to image capture or periodically through a specific routine.
- The hash script copies the drive image of the camera and compares it to the previously stored hash.
- If the hashes are the same, normal camera operations continue.
- If the hashes differ, the onboard camera drive contents are transferred off the camera and stored for future assessment.
- The payload drive is then overwritten with the original drive contents.
- Satellite operators are notified of mismatched hash alerts and will analyze the event.

4.2.1. Details

A corrupted picture image file can be detected, and a determination needs to be made whether this is an anomaly or a cyber intrusion. The camera's main software scripts and additional supporting resources onboard the camera platform will be assessed for modifications from the original deployment and production-ready scripts. The method of assessing for modifications will be done by an external security device onboard the payload platform that is connected to the camera via its micro-USB port. The external device will access the internal storage of the camera, then copy or scan the file contents, and compare the scanned scripts content with the baseline scripts/resources onboard the external device. The comparison process checks for code syntax, character counts, or file sizes changes with the original scripts/resources that are onboard the external device. If a modification is detected, the onboard camera scripts/resources will be removed and safely stored for future assessment and an original software copy will be put in its place.

4.2.2. Related CSF Subcategories

DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

SaveForests can implement a file checking solution that compares what is loaded on the satellite to the ground truth file that should be loaded on the payload.

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

The fault detection implementation being considered will be tested to demonstrate that it performs the following task:

- Compare on-orbit files to include software, data and information with known good files and report all inconsistencies.

4.3. Payload Encryption

Test use summary: SaveForests enabled payload data encryption and decryption practices including error detection, error correction, bulk link encryption and other transport layer protections.

Test Objective: Verify capability to encrypt data/commands before leaving payload.

Operational Process:

- Payload data are encrypted and transmitted to the ground station.
- Payload data are decrypted on the ground station terminal.
- Unencrypted data on the payload are deleted.

4.3.1. Details

- The payload transmits data through the host satellite’s bus and the host satellite’s infrastructure.
- An external device attaches to the camera to automatically encrypt all images and data before being transferred on the bus.
- Ground station collects transmission and sends camera data to data owner.
- Owner then decrypts the data with their key to view the unencrypted transmission.
- Data are protected in transit from the payload to the data owner.

Requirement: System shall provide secure transmissions to and from the camera payload using encryption, and other security safeguards, to provide availability, confidentiality, and integrity of camera data and image artifacts.

4.3.2. Related CSF Subcategories:

5. Summary

PR.DS-1: Data-at-rest is protected

The camera is capturing an image that is then encrypted while being stored. This encryption enables protection of the data prior to transmission via the host satellite through final delivery to the PCC.

PR.DS-2: Data-in-transit is protected

Plaintext data cannot be extracted from RF transmissions without the key.

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

Decryption of corrupted ciphertext will not be readable and easily detected as a loss of integrity.

PR.DS-5: Protections against data leaks are implemented.

Utilizing encryption keys, SaveForests enabled authorization procedures for protecting the confidentiality of payload information collected from the onboard camera.

Utilizing NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN), an organization can assess their cybersecurity posture based on a set of tailored perspectives within five high-level Functions; Identify, Protect, Detect, Respond, and Recover. As this document has shown, not all aspects of those Functions will be assessed in all instances; however, the process of adapting relevant facets yields a clearer understanding of an entity's standing. As the operational examples have shown, implementing CSF subcategories into the design of a system helps mitigate risk in operational processes, and the Profile supports the development of a management plan for cyber risk and resiliency in the hybrid satellite network ecosystem.

The CSF Profile for HSN develops a system that can be applied programmatically across multiple scenarios and deployments. This enables organizations to both integrate and retrofit current HSN ecosystems for bolstered security and situational awareness, as well as support development of future, more secure HSN implementations.

References

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

[NIST-IR-8270] Scholl M, Suloway T, (2023) Introduction to Cybersecurity for Commercial Satellite Operations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8270, https://doi.org/10.6028/NIST.IR.8270

[NIST-IR-8323r1] Bartock M, Lightman S, McCarthy J, Li-Baboud Y, Brule J, Reczek K, Meldorf K, Northrip D, Scholz A, Suloway T, (2023) Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8323r1, https://doi.org/10.6028/NIST.IR.8323r1

[NIST-IR-8401] Lightman S, Suloway T, Brule J, (2022) Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8401, https://doi.org/10.6028/NIST.IR.8401

[NIST-IR-8441] McCarthy J, Mamula D, Brule J, Meldorf K, Jennings R, Wiltberger J, Thorpe C, Dombrowski J, Lattin O, Sepassi S. (2023) Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8441, https://doi.org/10.6028/NIST.IR.8441

[NIST-SP-800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of July 18, 2023, https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-161r1] Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M. (2022) Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161, Rev. 1, https://doi.org/10.6028/NIST.SP.800-161r1

Appendix A. CSF Implementation

The five CSF Functions are divided into Categories that are further divided into Subcategories. The Subcategory is indicated by the index number. In the tables below, each Subcategory states the applicability of that subcategory to HSNs in general per the CSF HSN Profile, and through the implementation of the CSF HSN Profile, determinination of applicability to the fictitous SaveForests and its Partners stated in the far right column.

The CSF Identity Function (ID) has six Categories:

- Asset Management (AM)
- Business Environment (BE)
- Governance (GV)
- Risk Assessment (RA)
- Risk Management Strategy (RM)
- Supply Chain Risk Management (SC)

Table 7. Identity Function

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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. Successful interfaces will depend on a working knowledge of physical systems owned vs leased by external organizations as well as any constraints, performance requirements, and tolerances. Collaboration with external organizations is necessary to execute a physical inventory that spans organization locations and ownership. Be aware that in the HSN ecosystem, there are limits on the ability to execute a physical inventory (relative to an internal inventory).	**SaveForests:** The only physical SaveForests device on the satellite will be the payload itself. All physical interfaces with the payload will be through the satellite bus. (i.e., the payload does not have an alternate or independent RF transmission). Physical devices and systems at the PCC are also inventoried **Partner Organizations:** SatCo: The satellite and components (communication bus, RF transceiver, hosted payloads), and MOC devices and systems are inventoried

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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 inventory processes and procedures. Consider some level of automation.	**Payload owner Organization:** The payload software are micro python scripts that control image capture. The captured images are processed onboard along with any additional computational imaging processes and are stored either locally on the payload or streamed to the PCC storage using a communication protocol. A control script is created and pushed to the camera with all the functions and declarations necessary for it to run the mission. The commands and data to the payload are formatted on a virtual machine hosted on premises at the PCC. The virtual machine has a single purpose. Software package developed by payload manufacturer to parse telemetry data, mission data, and commands. **Partner Organizations:** SatCo: The software connection to the payload is through the Controller Area Network (CAN bus) and Serial peripheral interface (SPI) SatCo satellite interfaces. Data received from the payloads are processed by proprietary software that separates the data flows and forwards to a VPN interface in accordance with 802.3. Frame formatting software provided by a company that provides antennas as a service. The command formatting software for the satellite bus is a COTS product using the CAN Bus interface.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.AM-3: Organizational communications and data flows are mapped.	Consider policies that limit communication and data flows to only those necessary to fulfill the mission. Verify that data sources and recipients are authorized to send or receive data in accordance with the organization's policies. Flows may involve very different nodes such as a satellite, a terrestrial terminal, an operations center, or other platforms. In addition to the logical data flows, consider mapping physical ports / interfaces and document whether it is a common bus or somehow segregated.	**Payload owner Organization:** Logical data flow of communications, data, and commands with the payload are from the PCC through the MOC and host satellite to the payload. Logical data flow of mission data is from the payload through the host satellite and MOC to the PCC and SaveForests' headquarters. Logical data flow of payload state of health and telemetry is from the payload through the host satellite and MOC to the PCC. **Partner Organizations:** SatCo: Receives payload commands at the MOC from SaveForests, formats to CAN bus interface and forwards to the satellite. Can override a PCC command or deactivate the payload. Transmits payload commands through the Can Bus interface to the payload controller. Receives payload data via satellite RF downlink and ground stations.
ID.AM-4: External information systems are cataloged.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** This subcategory is related to information systems external to an organization, so it does not apply to SaveForests. **Partner Organizations:** SatCo: SatCo MOC software catalogue, particularly interfacing software with the PCC and any software that interacts with the communications to and from the satellite. Host satellite interface software catalogue, including a list of all legal commands able to send on the satellite bus. External parties SatCo relies on for normal operations that impact SaveForests, including the antenna communications provider SatCo uses for uplink and downlink transmissions.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.AM-5: Resources (e.g., 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 to include data and services provided externally. The HSN's prioritization effort often considers third-party relationships, agreements, and understandings between the participants.	**Payload owner Organization:** The priority and rationale in approximate order are: 1. On-orbit payload: Due to expense and single point of failure with respect to data collection. 2. Mission data repository: SaveForests' mission is to monitor and assess the progression and state of health of the world's forests. Maintaining the integrity and availability of the archives is critical to enable analysis. 3. Data handling, parsing, and processing software: Due to the volume and information density of the overhead collections, maintaining data handling is extremely important to SaveForests' mission to enable efficient and meaningful analysis. A failure in these functions may lead to permanent loss of information. 4. Payload data reception: Timely and uninterrupted data feeds strengthen the validity of any subsequent analysis. 5. Command Link formatting and transmission: The ability to re-task the overhead asset to focus on a different area or change some parameter of the collection benefits SaveForests' mission by providing agile data collection. **Partner Organizations:** SatCo: SatCo prioritizes the host satellite above any single payload being hosted. Other Partner Organization prioritizations of resources does not impact SaveForests' cybersecurity posture.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	Consider assigning cybersecurity roles and responsibilities to all participating organizations for the software, data, or components they manage. The roles and responsibilities of the external organization to the HSN are typically agreed upon in advance. Identify and resolve any inconsistencies or gaps in advance.	**Payload owner Organization:** Applicable. The complexity of the partnerships, MOUs, MOAs etc., increases with the number of independent entities involved. SaveForests has roles and responsibilities related to the payload, commands sent, PCC and data storage. **Partner Organizations:** SatCo: SatCo has roles and responsibilities related to the host satellite, MOC, and data transmission. SatCo is required to notify SaveForests should any command be overridden or should the payload be restricted or powered down. Payloads-R-Us is responsible to analyze on orbit faults.
ID.BE-1: The organization's role in the supply chain is identified and communicated.	Identify the role in the supply chain and consider any partners' role in the supply chain. Clearly communicate any corresponding expectations and requirements.	**Payload owner Organization:** SaveForests does not actively perform supply chain aspects of CSF and contracted for those services with Payloads-R-Us for the payload. **Partner Organizations:** SatCo' and Payloads-R-Us' role in the supply chain are defined in contractual documents.
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.	Placement in critical infrastructure is based on the service(s) provided (such as Communication services, Emergency services and others). 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 corresponding expectations. Capture the partner's requirements in addition to what will be provided to fulfill the operational objectives.	**Payload owner Organization:** SaveForests is not a part of the critical infrastructure. **Partner Organizations:** The mission is not part of the critical infrastructure.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	Prioritization of the mission objectives will facilitate the definition and evaluation of performance parameters for the HSN's service providers.	**Payload owner Organization:** Integrity of data repositories that store camera data, i.e., need high assurance that the data received by the payloads and stored on-premises are not corrupted. Accurate and timely information gathering and communication of forest overall health and biodiversity, for which the payload is an integral part for information gathering. Protection and availability of communication pathways to and from the payload and the mission data storage are important. Analyzing mission data, working with clients and partners, and all other business operations in support of SaveForests' mission. **Partner Organizations:** SatCo: SatCo has established and communicated the following organizational priorities to all its Partner Organizations. • Functionality and reliability of host satellite. • Ability to support all hosted payloads and communicate with satellite.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	Functions from external service providers critical to operations of the HSN are classified as such. Identify dependencies between organizations (hardware, software, data) to successfully define and execute the tasks.	**Payload owner Organization:** The following dependencies were identified by SaveForests: • SatCo to deliver commands to the payloads via its MOC. • SatCo to host payload. • Ground service element to provide antenna as a service to SatCo. • On-premises platform to house and execute mission and telemetry data parsing, analytics, and management functions. • Terrestrial-based internet service provider. • Local power grid. **Partner Organizations:** SatCo: SatCo has established the following dependencies. • GroundSyn to provide communication services to SatCo satellites. • SaveForests to provide commands for their payload. • On-premises systems to receive and communicate commands to the satellite. • On-premises systems to receive mission data from the satellite and forward all payload data to respective payload owners.
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	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. Clear and precise resilience requirements facilitate the definition of minimum performance parameters for HSN service providers.	**Payload owner Organization:** SaveForests' mission is to monitor and analyze the long-term health of the forests using relatively high thresholds and, therefore, has relaxed resiliency requirements. **Partner Organizations:** SatCo: SatCo has a resiliency requirement for each payload that can shut down the payload in emergency conditions when commanded by the satellite. SatCo's other resiliency requirements do not impact SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** SaveForests does not have a formal dissemination process but will need to address their needs and communicate with SatCo during the initial phases of the working partnership. **Partner Organizations:** SatCo: Adapts policy to conform with SaveForests needs as they are established and agreed upon.
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, partner or service provider to fulfill the pre-defined policies and performance parameters.	**Payload owner Organization:** In the event of a satellite degradation or outage: • SaveForests is responsible for bringing the payload back online. • SaveForests is responsible for isolation of the payload in the event of a cyber intrusion. • SaveForests shall resolve anomalous behavior from the payload within a specified time frame. Should the issue not be resolved, and the anomalous behavior impacts the satellite, the power and communications to the payload may be revoked. In the event of a cyber intrusion: • SatCo and SaveForests will notify the MOC or PCC within the specified timeframe. • SatCo and SaveForests in consultation with Payloads-R-Us will exchange data and analytic results in accordance with the MOU. • SaveForests is responsible for all measures to protect or patch the payload.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
		Partner Organizations: SatCo: SatCo is responsible for all matters related to satellite operation and provision of power to the payload. In the event of a satellite degradation or outage: • SatCo is responsible for notifying SaveForests when the payload was shutdown. In the event of a cyber intrusion: • SatCo and SaveForests will notify the MOC or PCC within the specified timeframe. • SatCo and SaveForests will exchange data and analytic results in accordance with the MOU. • SatCo is responsible for all measures to protect or patch the satellite.
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).	**Payload owner Organization:** SaveForests should review legal and regulatory requirements; however, their primary mission involves the monitoring and assessment of the health of forests and is not likely to include civil liberties or privacy issues. **Partner Organizations:** SatCo: SatCo provides bent pipe transponders for hosted payloads, and it is the responsibility of the mission and data owners to address issues associated with civil liberties and privacy issues.
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 components such as data vs bus vs payloads.	**Payload owner Organization:** SaveForests' governance does not directly address cybersecurity risks beyond what will be addressed by the risk management processes. **Partner Organizations:** SatCo: SatCo's governance addresses cybersecurity risks to the MOC.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.RA-1: Asset vulnerabilities are identified and documented.	In addition to traditional vulnerability management, consider focusing on the HSN interfaces and be aware of vulnerabilities inherited from the external service provider.	**Payload owner Organization:** The payload is vulnerable to: • Physical environment aspects, such as Dazzling, loss of power, communication interference, etc. • Any vulnerabilities inherited from SatCo's command link. • Any vulnerabilities inherited from SatCo's RF links (up and down) • Any vulnerabilities in the ground station infrastructure. • Any vulnerabilities inherited from other payloads hosted on the satellite. • Any vulnerabilities inherited from command protocols used on the satellite. • The software used at the PCC, which may contain vulnerabilities due to libraries, services, source code, configuration, or other sources. **Partner Organizations:** SatCo: the satellite is vulnerable to: • Physical environment aspects, such as kinetic impacts, loss of power, communication interference, etc. • Any vulnerabilities inherited from GroundSyn services. • Any vulnerabilities inherited from other payloads hosted on the satellite. • The software used at the MOC, which may contain vulnerabilities due to libraries, services, source code, configuration, or other sources.
ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources	Consider joining an organization or forum such as the Space ISAC.	**Payload owner Organization:** SaveForests is a small organization whose expertise is in biology and has limited resources. SaveForests does not actively search out or directly receive cyber threat intelligence during normal operation. **Partner Organizations:** SatCo: Receives cyber threat intelligence as part of its normal operations through manual research and cloud-based intelligence feeds in its ground-based cyber systems.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.RA-3: Threats, both internal and external, are identified and documented.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** Full blown threat analysis and documentation is resource intensive, and readers are advised to consult NIST IR 8286 (Integrating Cybersecurity and Enterprise Risk Management). Some of the threats that pertain to SaveForests' hosted payload and HSNs include but are not limited to: • RF attacks on the satellite host result in a loss of availability to the payload. • Dazzling or laser blinding result in a loss of image collection capability • Availability attacks to the terrestrial links from PCC to MOC result in a loss of availability to the payload. • Malware impacting on-premises storage may lead to an integrity loss of the mission data. • Data sniffing or manipulation, or both within the payload and in transmission. • Malware on payload impact delivery of mission data or camera operation. **Partner Organizations:** SatCo: Some of the threats that pertain to SatCo include but are not limited to: • Insider threats comprised of SatCo employees or SatCo's partner organization employees. • Availability attacks to uplink and downlink services.

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), Memorandum of Understanding (MOU), Service Level Agreement (SLA) or similar document.	**Payload owner Organization:** Obtaining precise and accurate likelihood information can be problematic but is required for meaningful risk analysis. The residual risk analysis is often limited due to the lack of sufficient likelihood data. When conducting actual impact and likelihood assessments, stakeholders are advised to analyze all threats in the context of the aspects of the mission affected for impact data and in the context of asset vulnerability for likelihood data. The following bullets Illustrate some considerations when assessing ID.RA-4: • The physical destruction or permanent loss of the payload has a critical impact on the mission due to being a single point of failure. The likelihood of a kinetic kill or destructive attack is low. • A loss of availability to the command link results in a loss of some data points, which degrades subsequent analysis but does not lead to mission failure or high loss. The likelihood of a successful availability attack or inability of SatCo to deliver a command to the payload is moderate. • A loss of availability of the mission downlink results in a loss of some data points, which degrades subsequent analysis but does not lead to mission failure or high loss. The intent for an adversary to deny the downlink to SaveForests is low, however, a downlink jamming attack intended for another mission would also deny SaveForests. The intent for an adversary to deny the downlink to other payload owners is unknown. The likelihood of a successful availability attack or inability to receive the mission downlink is indeterminant. • A loss of integrity to the archived mission data results in a loss of the ability to perform meaningful assessments and trend analysis. The impact of a degradation or loss of integrity to the mission data is very high. It could destroy the reputation of SaveForests, result in the inability to perform analysis and possibly mission

		failure. The likelihood of an integrity loss is moderate. • A loss of confidentiality to the mission data results in a partial loss of SaveForests' unique data collection. The impact is that SaveForests may lose some ground for providing information that may not be available to other competitors. The likelihood of a confidentiality loss is high. **Partner Organizations:** SatCo: SatCo's potential business impacts as it pertains to their business relationship with SaveForests: • Degradation or denial of service to the satellite and all hosted payloads due to individual payload actions. • Impact or degradation of operations performed at the MOC. SatCo's other potential business impacts are not related to SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** Likelihood and impact determinations can be challenging but is vital for determining risks associated with threats and vulnerabilities. When performing risk determinations, it is recommended stakeholders analyze risks using CTI for threats and vulnerabilities, in the context of the affected mission aspects for impacts, and in the context of asset and system vulnerability for likelihood. The following bullets illustrate some example considerations of SaveForests when assessing ID.RA-5: • Physical destruction of the host satellite has a low likelihood but extreme impact. • Command link intrusion has a moderate impact and low likelihood due to SatCo's protection of the command link. • Downlink jamming has a moderate impact, but the likelihood requires additional knowledge of other payloads. • Passive collection of mission data has a very high likelihood. Impact to the primary SaveForests' mission is low, but the impact to SaveForests' future customers may be higher. • Due to extremely high impact to the mission, risks to the camera payload and ability to collect mission data were determined to be severe. • Due to impact to mission data availability, risks to the PCC storage and payload communication were determined to be moderate. • Due to SatCo utilizing unencrypted downlinks, SaveForests determined the risk to confidentiality of mission data to be high. **Partner Organizations:** SatCo: SatCo's determination of risk is managed through contractual agreements with partner organizations and service providers.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.RA-6: Risk responses are identified and prioritized.	Consider 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), that could result in a possible failure to fulfill a partner agreement/contract element.	**Payload owner Organization:** Risk responses include decisions such as accept the risk, mitigate the risk, or transfer the risk. • SaveForests has rejected the risk to total loss of payload in the event of satellite collision or other total loss of satellite functionality and transferred the risk by purchasing an insurance policy. • SaveForests accepted the risk of a command link intrusion due to the command link protections in place by SatCo. • SaveForests will mitigate the risk due to passive collection by implementing confidentiality measures in the data feeds. • SaveForests will mitigate the risk from a backdoor by implementing measures that assure authorized commands. • SaveForests rejected the risk of lengthy communication downtime and will enter negotiations with SatCo to mitigate. • SaveForests rejected the risk to loss of PCC, equipment, and data due to natural or man-made cause and will transfer the risk to an insurance company. **Partner Organizations:** SatCo: SatCo’s command link protections minimize the risk of a command link attack against SaveForests. SatCo accepted the risk of a downlink jammer and passive collection, which requires SaveForests to address directly. SatCo accepted the risk of a backdoor in one or more payloads, which requires SaveForests to address directly.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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, especially if a collaborative effort is needed to mitigate an attack, vulnerability, or otherwise manage the residual risk.	**Payload owner Organization:** SaveForests and SatCo will need to have insight and agree to each other's risk management processes. **Partner Organizations:** SatCo: SaveForests and SatCo will need to have insight and agree to each other's risk management processes.
ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	In addition to intra-organizational segmentation and risk management, HSNs should consider expressing their risk tolerance to external component and service providers. The HSN's risk tolerance is typically expressed as performance parameters and requirements.	**Payload owner Organization:** SaveForests can tolerate some C2 outage to the payload while SatCo is risk averse to any threat to the spacecraft. Differences in the risk tolerance may require one or more stakeholders to modify or caveat their risk response. **Partner Organizations:** SatCo: SatCo cannot tolerate risks resulting in the total loss of satellites or MOC services. Differences in risk tolerances between partner organizations may require one or more organizations to modify or caveat risk responses.
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.	**Payload owner Organization:** SaveForests is not a part of the critical infrastructure, however, other payloads on SatCo may be. The potential impact to other payloads (and potentially on the critical infrastructure) may impact SaveForests' tolerance. **Partner Organizations:** SatCo: SatCo is not a part of critical infrastructure, any payload hosted by SatCo that is part of critical infrastructure is up to that individual organization to determine and communicate risk tolerances.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** SaveForests is a small organization whose expertise is in biology and has limited resources. SaveForests does not have an established cyber supply chain risk policy but, instead, performs ad hoc assessments for each supply chain purchase. **Partner Organizations:** SatCo: SatCo has a cyber supply chain risk management process and applies it to dealings with SatCo's supply chain organizations.
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.	**Payload owner Organization:** SaveForests performs an ad hoc assessment for each supply chain purchase utilizing the cyber supply chain risk management structure outlined in NIST-SP-800-161, particularly Appendix A Family: System and Services Acquisition. **Partner Organizations:** Payloads-R-Us: As the Original Equipment Manufacturer (OEM) of the camera payload SaveForests is using, Payloads-R-Us and SaveForests fully coordinated and communicated during the acquisition process of the camera payload to ensure correct and complete functionality and cybersecurity concerns are addressed.
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.	**Payload owner Organization:** SaveForests is a small organization and does not have longstanding supply chain partners, so they do not have contractual agreements in place. **Partner Organizations:** Both SatCo and Payloads-R-Us have longstanding supply chain partners for their on-orbit components and have contractual language and agreements with all appropriate partners regarding the cyber posture and cyber supply chain risk management.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluation to confirm that they are meeting their contractual obligations.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** SaveForests is a small organization and does not have longstanding supply chain partners, so they do not perform routine supplier and third-party partner assessments. **Partner Organizations:** SatCo: SatCo performs tests and assessments regarding their suppliers regarding contractual obligations periodically and prior to contract renewal.
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** SaveForests is a small organization and does not have longstanding supply chain partners, so they do not perform planning and testing activities with suppliers and third-party providers. **Partner Organizations:** SatCo: SatCo conducts response and recovery planning with suppliers for all terrestrial systems but does not conduct any tests with orbiting satellites.

The CSF Protect Function (PR) has six Categories:

- Access Control (AC)
- Awareness and Training (AT)
- Data Security (DS)
- Information Protection Processes and Procedures (IP)
- Maintenance (MA)
- Protective Technology (PT)

Table 8. Protect Function

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** Interactions with the payload are strictly limited to a subset of SaveForests' personnel who are authorized to command the satellite. The SatCo MOC authenticates with the PCC. Access to the PCC is strictly managed by SaveForests. The telemetry and mission data are downlinked to the MOC and then transported directly to PCC. SaveForests implements role-based access control to the mission and telemetry data stored on-premises at PCC. **Partner Organizations:** SatCo: SatCo issues and manages credentials and access to the MOC.
PR.AC-2: Physical access to assets is managed and protected.	Emphasize managing physical access to assets by external organizations.	**Payload owner Organization:** PCC access is reserved for SaveForests' employees, requiring additional credentials for access. **Partner Organizations:** SatCo: MOC access is reserved for SatCo employees and a select few partners, both requiring additional credentials.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.AC-3: Remote access is managed.	Critical for HSNs. In addition to remote access for normal operations, consider access to external operators, users, and other personnel. Consider implementation of agile remote access procedures that are in accordance with the agreements between partners' and the organization's contingency plans.	**Payload owner Organization:** Access to, formatting, processing, and other interactions with the PCC' and SaveForests' data are done through virtual machines hosted on-premises. **Partner Organizations:** SatCo: Remote access to the MOC and SatCo assets are managed by SatCo.
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.	**Payload owner Organization:** SaveForests maintains separation of duties and least privilege by defining the capabilities of the virtual machines, and access to the virtual machine is granted in accordance with the role of the authenticated user. Access permissions and authorization to interact with the payload and MOC are only granted to a managed group of SaveForests' personnel. **Partner Organizations:** SatCo: SatCo incorporates the principles of least privilege and separation of duties to access permissions granted related to the MOC and to communications with satellites.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** SaveForests accesses its data and virtual machines via a service provider and does not directly control the management and state of health of the network. Save Forests does not control or manage the RF emanations from SatCo to the ground. SatCo does not segregate or segment the network from the hosted satellite, so information from SaveForests, SatCo, and the third commercial entity all traverse the same pathways. This poses a risk to SaveForests and the commercial entity if SatCo's network to the satellite is compromised or the communications are being recorded by a malicious actor. **Partner Organizations:** SatCo: SatCo does not perform network segmentation for communications with the satellite.
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.	**Payload owner Organization:** SaveForests uses a third-party service for certificate management with it set up to require a username and password for normal network access and an additional SMS verification code for access to the PCC network. **Partner Organizations:** SatCo: SatCo uses software cryptographic authentication tokens for access to the MOC.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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).	Consider 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 may be a priority. Evaluate the risks and implement adequate controls in accordance with the diversity of the HSN. Consider controls such as multi-factor authentication.	**Payload owner Organization:** Interactions with the SaveForests database requires an SMS verification in addition to a username and password. **Partner Organizations:** SatCo: The MOC at SatCo required the use of a token associated with a particular computer in addition to a username and password.
PR.AT-1: All users are informed and trained.	HSN operators should consider that staff receive adequate cybersecurity training, especially on assets not internal to the organization.	**Payload owner Organization:** SaveForests has all users take security training during onboarding and refresher training every 5 years. Additional training is required for users with access to the PCC, including annual refreshers. **Partner Organizations:** SatCo: All non-SatCo users with access to the MOC are given training prior to being granted access to the MOC and every 6 months while having access.
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 policies.	**Payload owner Organization:** SaveForests has created policies regarding roles and responsibilities for personnel granted access to the payload and/or mission data and includes review of role-specific policies as part of training for each role. **Partner Organizations:** SatCo: SatCo has created policies regarding roles and responsibilities for personnel granted access to the payload and/or mission data and includes review of role-specific policies as part of training for each role.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	Consider agreements in advance with all partners to clearly define roles and responsibilities and performance parameters that are measurable and verifiable.	**Payload owner Organization:** SaveForests understands that SatCo may deny access or isolate the payload if there is a reasonable expectation of a risk to the satellite from the payload. SaveForests understands that they are solely responsible for the analysis and return of the payload to proper working order. **Partner Organizations:** SatCo: SatCo understands their roles and responsibilities regarding SaveForests, including as it relates to providing the services necessary for SaveForests' payload.
PR.AT-4: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	The HSN will require shared usage across the elements of the HSN. Senior executives from the different organizations should agree upon and ensure buy-in within their organization so that the terms of the agreements will be met.	**Payload owner Organization:** SaveForests has documented and communicated the roles and responsibilities with SatCo. **Partner Organizations:** SatCo: SatCo has documented and communicated the roles and responsibilities with SaveForests and all other companies whose payloads are being hosted.
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** SaveForests has documented and communicated the roles and responsibilities to their physical and cybersecurity personnel. **Partner Organizations:** SatCo: SatCo has documented and communicated the roles and responsibilities to their physical and cybersecurity personnel.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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 should be communicated and written into policy.	**Payload owner Organization:** SaveForests relies on embedded payload encryption to protect data-at-rest. PCC implements standard boundary layer protections (e.g., firewall, network intrusion detection). **Partner Organizations:** SatCo: SatCo protects SatCo data at the MOC using standard boundary layer protections (e.g., firewall, network intrusion detection. SatCo forwards all payload generated data to the payload owners without storing it.
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, Frequency Hopping Spread Spectrum, or other transmission security measures should be considered.	**Payload owner Organization:** SaveForests' PCC uses encrypted communications for command uplink to the payload. **Partner Organizations:** SatCo: Uplink commands are encrypted.
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	Consider policies and procedures for the removal, transfer, and disposition of assets between internal and external organizations that maintain confidentiality and integrity.	**Payload owner Organization:** SaveForests manages the assets on-premises at the PCC in accordance with their asset management policies. **Partner Organizations:** SatCo: The disposition of the payload was transferred to SatCo.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.DS-4: Adequate capacity to ensure availability is maintained.	In addition to the availability requirements for the organization's business needs, determine what level of availability needs to be maintained so that the requirements of the partner organizations are fulfilled in accordance with any MOU, SLA, or other agreements.	**Payload owner Organization:** SaveForests has a QoS agreement with SatCo for minimum communication uptime with the host satellite and a maximum downtime for loss of communications. **Partner Organizations:** SatCo: SatCo has a QoS agreement with GroundSyn for minimum communication uptime with SatCo satellites and a maximum downtime for communications.
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.	**Payload owner Organization:** Other than authentication / authorization procedures, no data leak protections are in place. The mission and telemetry data from the payload are plaintext and downlinked to SatCo, then SatCo parses the data from the satellite's bus and other payloads and forwards to a PCC storage facility. **Partner Organizations:** SatCo: SatCo does not implement data leak protections, other than authentication / authorization processes.
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** Analysis and reports generated by SaveForests are cryptographically signed. SaveForests generates a hash after the data received from the MOC is parsed. **Partner Organizations:** SatCo: SatCo verifies software and firmware prior to use but does not take any information integrity actions for communications.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.DS-7: The development and testing environments are separate from the production environment.	Not directly applicable to HSN.	**Payload owner Organization:** SaveForests utilizes advanced data processing as part of their forest health assessment and to better provide functionality to their customers. SaveForests has separate development and testing environments for their advanced data processing software. Each version of this software must pass testing and inspection when transitioning out of testing into development and out of development into production environments. **Partner Organizations:** SatCo: SatCo does not have separate testing and development environments as they do not create any software or hardware used on their satellites or MOC in-house.
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	Consider verification of the integrity for any hardware required to make the HSN system operational. Be aware of and consider the challenges associated with verifying hardware built by different vendors. Consider the use of independent assessors or third-party verification during the operational phase.	**Payload owner Organization:** Payloads-R-Us implemented a checksum procedure when the payload is activated that will alert the PCC in the event of a failure. **Partner Organizations:** SatCo: SatCo performs hardware integrity checks of the satellite during the boot phase and for diagnostic reasons.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** The command formatting unit at the PCC was delivered to SaveForests by Payloads-R-Us. It's a single purpose device on a SELinux OS. The device can be connected to the MOC via a network connection but does not have software for email, web-browsing, etc. The mission data parsing software was provided by Payloads-R-Us vendor. SaveForests nonanalytic software, reporting, business, and other software are COTS products for word processing, spreadsheets, presentations, relational databases using the default configurations. **Partner Organizations:** SatCo: SatCo maintains a golden image base configuration file for every satellite at the MOC.
PR.IP-2: A System Development Life Cycle to manage systems is implemented.	An SDLC 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.	**Payload owner Organization:** SaveForests' mission statement is to analyze data to monitor the health of forests. System development is beyond the scope of their mission. **Partner Organizations:** SatCo: SatCo implements a system development life cycle for each satellite.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.IP-3: Configuration change control processes are in place.	Organizations should employ configuration change control consistent with the software 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.	**Payload owner Organization:** Prior to any configuration changes to the payload, SaveForests will present to their senior management the purpose of the change, Payloads-R-Us will be consulted regarding impacts of the change and SatCo will be informed and will approve of the changes. **Partner Organizations:** SatCo: SatCo must approve any configuration change on the satellite or hosted payloads prior to the change occurring.
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.	**Payload owner Organization:** SaveForests implemented RAID level 1 for the mission data and telemetry data. SaveForests has offsite backup that is updated daily for all its operational data. **Partner Organizations:** SatCo: SatCo implements RAID level 1 storage at the MOC for telemetry and command data.
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Applicable to HSN and complicated by third-party owned components (hardware, software, applications, etc.) No HSN-specific concerns.	**Payload owner Organization:** The command formatting unit for the payload is in a separate room that requires a keycard for access. The servers are located in a separate facility and physical access requires a keycard and is limited. **Partner Organizations:** SatCo: Physical access to the MOC is limited and requires a SatCo company employee to escort. The servers are in a separate room and require a SatCo company employee to escort.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.IP-6: Data are destroyed according to policy.	Consider third-party data retention and proper disposal. Likewise, external organizations should consider destroying data that are no longer required for HSN operations, according to pre-arranged agreements and policies.	**Payload owner Organization:** A copy of the payload's telemetry data is delivered to SatCo and archived for the life of the satellite. SaveForests retains the mission data indefinitely. SaveForests retains reports and analysis for 12 months after delivery. Sensitive data are cryptographically overwritten. An MOU between SatCo and SaveForests requires deletion of SaveForests' mission data within 30 days of delivery via electronic media. **Partner Organizations:** SatCo: SatCo retains a copy of telemetry and command data indefinitely. SatCo deletes SaveForests' mission data in accordance with the MOU.
PR.IP-7: Protection processes are improved.	Consider the ramifications of any HSN protection process changes and how they relate to the service providers protection process.	**Payload owner Organization:** Protection processes are re-evaluated on an annual basis and if necessary modified and improved in accordance with changes in SaveForests' client base or changes in its business objectives. **Partner Organizations:** SatCo: SatCo evaluates and improves protection processes.
PR.IP-8: The effectiveness of protection technologies is shared.	Effectiveness of protection technologies is shared with partner organizations in a manner that is consistent with pre-existing agreements while protecting the organization's equities.	**Payload owner Organization:** SaveForests and SatCo have an MOU to share payload incident reports to include remediation steps taken to return to proper working order. **Partner Organizations:** SatCo: SaveForests and SatCo have an MOU to share payload incident reports to include remediation steps taken to return to proper working order.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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 are complicated by the diversity of the partners' information, geographic separation, and interfaces between the HSN and its service providers.	**Payload owner Organization:** Recovery of the payload and returning to proper working order is SaveForests' responsibility and any recovery plan must be reviewed and approved by SatCo. **Partner Organizations:** SatCo: SatCo may isolate or power down the payload at its discretion should there be a risk to the satellite bus. Recovery of the satellite and returning it to proper working order is SatCo's responsibility.
PR.IP-10: Response and recovery plans are tested.	Consider including partner organizations when testing response and recovery plans. Full-scale testing 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.	**Payload owner Organization:** Payloads-R-Us makes a digital twin available to SaveForests for purposes of testing. **Partner Organizations:** SatCo: SatCo tests response and recovery plans after every update to the plans.
PR.IP-11: Cybersecurity is included in human resources in practices (e.g., deprovisioning, personnel screening).	Applicable, no HSN-specific considerations.	**Payload owner Organization:** SaveForests provisions access credentials to all employees during onboarding and deprovisions them upon separation. **Partner Organizations:** SatCo: SatCo provisions access credentials to all third parties requiring access to the MOC upon completion of training and deprovisions when no longer required.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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 can be applicable.	**Payload owner Organization:** SaveForests' vulnerability management plan for the payload is coordinated with SatCo and is supported by the payload vendor. SaveForests' vulnerability plan for non-payload/satellite-specific considerations are already implemented and follows industry best practices. SaveForests relies on the automatic update functions provided by COTS products for software and IT. **Partner Organizations:** SatCo: SatCo coordinates payload vulnerability management plans with SaveForests and each payload owner.
PR.MA-1: The maintenance and repair of organizational assets are performed and logged with approved and controlled tools.	Directly applicable for HSN firmware and software considerations but not directly applicable to other assets.	**Payload owner Organization:** SaveForests archives all maintenance logs for the payload for the duration of the payload's operational life. All maintenance tools are provided by Payloads-R-Us and approved by SatCo. **Partner Organizations:** SatCo: SatCo approves all maintenance tools for the satellite and payloads prior to implementation.
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** Remote maintenance of the servers storing the mission data is prohibited. Otherwise, remote maintenance is done over an encrypted channel using TFA and authorization. **Partner Organizations:** SatCo: SatCo logs and performs maintenance on all assets using encrypted channels and MFA.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
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. Consider policies that promote audit log sizing, and aging that meet industry best practices.	**Payload owner Organization:** All logs pertaining to the payload are formatted in accordance with a standard agreed upon with SatCo. All IT logs are formatted in accordance with the format defined by a COTS security information and event management (SIEM) tool. **Partner Organizations:** SatCo: SatCo has created and manages standards for logs pertaining to payloads, which payload owners agree to and abide by.
PR.PT-2: Removable media are protected, and their use is restricted according to policy.	HSNs may need to support using removable media to exchange data between partners and other organizations.	**Payload owner Organization:** Removeable media may be used by the PCC for purposes of uploading a script of commands or for rekeying the payload. Removable media for the PCC or server room may not be used for other purposes and must be physically secured. **Partner Organizations:** SatCo: SatCo protects and restricts removable media use at the MOC by disabling USB ports on all but a select few endpoints and requiring a security scan of the removable media before and after connection to SatCo systems.
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.	**Payload owner Organization:** The PCC command formatting unit is a single purpose device, and loading of other programs is prohibited. **Partner Organizations:** SatCo: The MOC incorporates the principle of least functionality by having dedicated virtual environments for each satellite, reducing the functionality of each one to only what is required for that satellite.

CSF Subcategory	CSF Profile Applicability for HSNs	Applicability to SaveForests and Partner Organizations
PR.PT-4: Communications and control networks are protected	Multiple organizations may share a common infrastructure, consider the proper controls to meet organizational policies.	**Payload owner Organization:** Commands from the PCC to the MOC are encrypted and require two-factor authentication (2FA). Access to the database requires authentication and role-based authorization **Partner Organizations:** SatCo: SatCo incorporates 2FA for communications sent through the MOC.
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.	**Payload owner Organization:** SaveForests' mission is to monitor and analyze trends associated with the health of forests. Short term outages are not mission critical, and the need to operate through adverse situations is minimal. The imagery provided by the payload is a single point of failure, however, the occasional absence of imagery data will not significantly degrade the analysis. The need to operate through adverse situations is minimal. **Partner Organizations:** SatCo: SatCo has satellite mechanisms for redundant power and communication to all critical systems. SatCo has resilience of communications to the satellite through its contract with GroundSyn.

The CSF Detect Function (DE) has three Categories:

- Anomalies and Events (AE)
- Security Continuous Monitoring (CM)
- Detection Processes (DP)

Table 9. Detect Function

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	It is especially important to focus on the expected (or normal) data and information flow at the ingress and egress of the interfaces (including wired, RF and virtual). 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.	**Payload owner Organization:** SaveForests' cybersecurity posture is improved through understanding and recording the normal and expected data flows through their systems and networks. This helps enable SaveForests to detect abnormal or malicious behavior easier and can help restore functionality in the event of an attack. **Partner Organizations:** SatCo: SatCo has an established baseline of network operations and expected data flows, which SatCo uses to determine abnormal behavior and communicate those findings appropriately.
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	Review and analyze detected events within the HSN system to understand the characteristics (e.g., source, data error statistics, duration, frequency, and location) of anomalous events. Distinguishing between potentially harmful events and normal operations requires an understanding of attack targets and methods. Be able to predict the level of harm based on event analysis. Consider 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.	**Payload owner Organization:** SaveForests implemented a COTS analytic tool to analyze the raw data. The COTS tool has a feature that analyzes its customer data to assess methods from a global perspective to update their signature and analytic packages. **Partner Organizations:** SatCo: SatCo's detection and analysis methods do not impact SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	Data from multiple sources 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, and audits. Monitor the network, physical access, human-machine interface activity, user reports, and administrator reports. Standards-based data formatting and serialization promotes communication, interoperability, and exchange 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 (such as open source, industry forums, user groups and others).	**Payload owner Organization:** SaveForests implemented COTS firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). The COTS product includes an analytic package that integrates data feeds from the products. **Partner Organizations:** SatCo: SatCo's event data collection practices do not impact SaveForests.
DE.AE-4: 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.	**Payload owner Organization:** SaveForests implemented a COTS analytic tool to analyze the raw data to determine the impact of internet protocol (IP) network events. SaveForests contracted with the payload vendor to analyze the raw telemetry from the payload to detect and analyze the impact of on-orbit events. **Partner Organizations:** SatCo: SatCo's impact determination does not impact SaveForests.
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.	**Payload owner Organization:** SaveForests set thresholds for the payload to include a loss of telemetry data for a period greater than 45 minutes, a failure to acknowledge two or more consecutive commands, and a deviation of the camera orientation from the last acknowledged position. **Partner Organizations:** SatCo: Incident alert thresholds that impact the payloads established by SatCo are communicated with SaveForests.

CSF Subcategory	**CSF Profile Applicability to HSNs**	**Applicability to SaveForests and Partner Organizations**
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, agreed upon time.	**Payload owner Organization:** SaveForests uses a COTS IDS to monitor network traffic at the boundary. SaveForests uploads the payload telemetry to Payloads-R-Us on a weekly basis. The vendor is under contract to produce weekly summaries and to notify SaveForests of all events where the thresholds were exceeded. **Partner Organizations:** SatCo: SatCo's specific network monitoring efforts do not impact SaveForests, if SatCo provides the levels of service agreed upon in the MOA.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	Not directly applicable to HSNs.	**Payload owner Organization:** SaveForests has badge readers for physical access to the PCC. There are no detection capabilities for physical access to the payload. **Partner Organizations:** SatCo: SatCo uses badge readers for physical access to the MOC. There are no detection capabilities for physical access to the satellite.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** SaveForests monitors user activity to include log in, failed log in, attempts to access files, internet activity. The log data are analyzed on a weekly basis, and changes in behavior are flagged. **Partner Organizations:** SatCo: SatCo performs personnel monitoring of all individuals with access to the MOC.
DE.CM-4: Malicious code is detected.	Given the increased level of access and privileges that may be provided externally, it is essential to detect malicious code. Consider multi-layered detection strategies.	**Payload owner Organization:** For user accounts, SaveForests leases COTS malware detection service that continuously runs in the background and performs a full scan weekly. **Partner Organizations:** SatCo: SatCo's malicious detection activities do not impact SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** SaveForests uses a COTS IDS that according to the vendor, detects potentially malicious mobile code. **Partner Organizations:** SatCo: SatCo's unauthorized mobile code detection activities do not impact SaveForests.
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.	**Payload owner Organization:** SaveForests uses SatCo for all communications to their payload, for which SaveForests monitors SatCo for potential cybersecurity events by correlating commands sent from the PCC with the commands acknowledged by the payload. **Partner Organizations:** SatCo: SatCo only monitors GroundSyn for communication outages.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	Focus on data flow discrepancies, unauthorized connections, and access points. Monitoring may include RF detection and direction finding.	**Payload owner Organization:** SaveForests monitors connections using a COTS firewall with a deny by default configuration. Only users with admin privileges may install software. **Partner Organizations:** SatCo: SatCo monitors connections to the MOC, only allowing authorized users to make connections after verifying their identity.
DE.CM-8: Vulnerability scans are performed.	Applicable, no HSN-specific considerations.	**Payload owner Organization:** SaveForests performs vulnerability scans of their PCC and payload systems regularly for vulnerabilities. For the payload this is primarily done through configuration and system checks to ensure no unexpected changes have been made, and for the PCC this follows standard IT vulnerability scanning practices. **Partner Organizations:** SatCo: SatCo's vulnerability scanning activities do not impact SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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 performance criteria are defined when feasible. Understand HSN service provider 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.	**Payload owner Organization:** SaveForests and SatCo have an MOU in place requiring that the following breaches are to be disclosed; Unauthorized access to the PCC or MOC. **Partner Organizations:** SatCo: SatCo's discloses unauthorized access to the PCC or MOC to SaveForests.
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.	**Payload owner Organization:** SaveForests and SatCo are responsible to deliver the results of audit logs on a biweekly basis and report changes in baseline behavior, changes in traffic patterns and changes in offered traffic load. **Partner Organizations:** SatCo: SatCo is responsible to deliver audit log results that are directly related to the payloads on a biweekly basis to SaveForests.
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.	**Payload owner Organization:** A clause in the SaveForests and SatCo MOU requires an annual red-team exercise on an annual basis to test the detection processes and procedures. **Partner Organizations:** SatCo: SatCo's MOU with SaveForests requires annual red team exercises to test detection processes and procedures.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
DE.DP-4: Event detection is communicated	Appropriate responses require event detection information in cyber-relevant time at the HSN interfaces. Definition of thresholds and other criteria in advance will facilitate timely detection. 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 should have prearranged information sharing agreements.	**Payload owner Organization:** SaveForests communicates with SatCo when events impacting or related to SatCo are detected; these include when communication with the payload is not available for a period greater than (some number of hours), if the camera orientation is inconsistent with the last known state, or if the camera telemetry indicates power consumption that exceeds the thresholds defined in the MOU between SaveForests and SatCo. **Partner Organizations:** SatCo: SatCo communicates to SaveForests detected events impacting SaveForests' payload or the PCC.
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.	**Payload owner Organization:** A clause in the SaveForests and SatCo MOU requires a battle damage assessment at the conclusion of the red team exercise and application of lessons learned where appropriate. **Partner Organizations:** SatCo: SatCo's MOU with SaveForests requires incorporating lessons learned for existing detection processes from the annual red-team exercises.

The CSF Respond Function (RS) has five Categories:

- Response Planning (RP)
- Communications (CO)
- Analysis (AN)
- Mitigation (MI)
- Improvements (IM)

Table 10. Respond Function

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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.	**Payload owner Organization:** In occordance with (IAW) the pre-defined thresholds, SaveForests initiates the response plan and informs SatCo IAW the MOU.
RS.CO-1: Personnel know their roles and order of operations when a response is needed.	Consider personnel training that 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.	**Payload owner Organization:** SaveForests has defined the response team leaders and participants by role, provides web-based training modules (frequency and duration is role-dependent) and exercises the response in conjunction with annual red team exercises.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
RS.CO-2: Incidents are reported consistent with established criteria.	Ensure that cybersecurity events that exceed a predetermined threshold are reported across stakeholders.	**Payload owner Organization:** SaveForests self-reports to SatCo breaches in confidentiality at the PCC or payload anomalies that involve use of power or bandwidth in excess of the SLA between SatCo and SaveForests. SatCo self-reports to SaveForests breaches in confidentiality at the MOC or satellite anomalies involving degradation of service or impact to SaveForests' payload in accordance with the SLA between SatCo and SaveForests. High-impact incidents are to be reported within 12 hours of detection. Other incidents are to be reported within two business days. Incidents that involve ransomware are reported to the internet service provider. Incidents that involve a breach of personal identification information (PII) are reported to the affected parties within one business day.
RS.CO-3: Information is shared consistent with response plans.	Timely information exchange within and between organizations improves the overall efficiency of incident response. Exchange information with external stakeholders in accordance with prearranged agreements, thresholds, and formats to ensure that obligations are met.	**Payload owner Organization:** SaveForests self-reports to SatCo breaches in confidentiality at the PCC or payload anomalies that involve use of power or bandwidth in excess of the SLA between SatCo and SaveForests. **Partner Organizations:** SatCo self-reports to SaveForests breaches in confidentiality at the MOC or satellite anomalies involving degradation of service or impact to SaveForests' payload in accordance with the SLA between SatCo and SaveForests.
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.	**Payload owner Organization:** Upon request, SaveForests grants SatCo cybersecurity analysts access to the PCC for the duration of the incident. SaveForests grants the payload vendor regular access to the payload.

CSF Subcategory	**CSF Profile Applicability to HSNs**	**Applicability to SaveForests and Partner Organizations**
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.	**Payload owner Organization:** SaveForests is a small organization whose expertise is in biology and has limited resources. SaveForests does not participate in cybersecurity or satellite security forums.
RS.AN-1: Notifications from detection systems are investigated.	Investigate cybersecurity-related notifications generated by the anomaly detection systems.	**Payload owner Organization:** SaveForests' requires a review of internally generated notifications within 24 hours to determine if the event should be elevated to an incident. SaveForests requires a review of notifications from SatCo within 24 hours to determine if the event should be elevated to and incident.
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), or the end-user community.	**Payload owner Organization:** Incidents are reported to department heads that include the type of the incident (such as a loss of availability, the loss of data files, the presence of unauthorized actors) and a projected duration of the incident. Department heads are required to assess the impact to their departments within 5 days of receipt. The departmental data to assess the impact to SaveForests and to SatCo.
RS.AN-3: Forensics are performed.	Consider performing forensics on cyber events to aid in root cause analysis and residual effects. Some of the relevant data may be on a host system or service provider and the HSN's forensic team may not have access to all the relevant data.	**Payload owner Organization:** SaveForests has the ABC cyber-consulting firm on retainer to perform preliminary forensic analysis for cyber-related incidents to determine root cause analysis. SaveForests has an MOU with the payload manufacturer to perform forensic analysis for on-orbit events and incidents.
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.	SaveForests assigns incidents in one of three categories based on the urgency (i.e., how rapid of a response is required) and the impact to the SaveForests mission. SaveForests also assigns incidents of three categories based on the urgency and impact of the incident on SatCo.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, security researchers).	Consider establishing processes for responding to disclosed vulnerabilities. These processes are especially important when the vulnerability affects the HSN interfaces or data flows.	SaveForests' vulnerability response and management does not go beyond the processes defined within the protect function.
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. Consider processes to enable automated response capabilities to reduce response time for active threats. Consider technologies such as artificial intelligence or machine learning to hasten the response.	Incidents that involve a compromise to the integrity of the archived imagery data are contained by initially denying all access, then updating access to archived data for the duration of the incident. Incidents that involve corrupted or untrusted imagery data are contained by holding all incoming imagery on a temporary drive and investigating the data for evidence of corruption prior to loading it to the databases for the duration of the incident. Incidents that involve unauthorized remote access are contained through renewing all connections periodically for the duration of the incident. Incidents that involve unauthorized remote control or remote code execution are contained through severe restrictions placed on internet access and traffic until access controls are updated and the system is confirmed clear of unauthorized remote connections.
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.	SaveForests' response plans focus on mitigating cybersecurity incidents when they occur and updating or adapting cyber posture to mitigate future incidents from occurring.
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	Risk assessments 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.	SaveForests documents or mitigates risks as they are made aware of them; however, SaveForests is a small organization with limited resources, so they do not actively search for new vulnerabilities.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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.	SaveForests has the ABC cyber-consulting firm on retainer. If the response to the incident did not meet the satisfaction of the department heads within SaveForests, then a damage and response assessment with ABC will be initiated and any lessons learned presented by ABC will be considered.
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.	SaveForests' response strategies will be updated in conjunction with the incorporations of lessons learned should it be determined that the current strategy is sub-optimal.

The CSF Recover Function (RC) has three Categories:

- Recovery Planning (RP)
- Improvements (IM)
- Communications (CO)

Table 11. Recover Function

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
RC.RP-1: 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. Consider system testing to verify the systems are restored to proper working state.	**Payload owner Organization:** SaveForests has recovery plans ready for execution at any time for incidents involving the payload and PCC but does not have document recovery plans for other incidents. **Partner Organizations:** SatCo: SatCo executes recovery plans in conjunction with SaveForests when coordination is required, otherwise SatCo recovery activities do not involve SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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 during plan implementation, execution, and testing.	**Payload owner Organization:** SaveForests updates existing recovery plans (to reflect lessons learned from the cybersecurity incident and related response and recovery activities) as part of the recovery plan, but not as a routine aspect of SaveForests' cyber posture. **Partner Organizations:** SatCo: SatCo's efforts to incorporate lessons learned do not involve SaveForests.
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.	**Payload owner Organization:** SaveForests updates existing strategies at the same time they update recovery plans. Being a smaller organization, SaveForests' recovery strategies are entirely encapsulated by the recovery plans. **Partner Organizations:** SatCo: SatCo's strategy updates do not involve SaveForests.
RC.CO-1: Public relations are managed.	Coordination among stakeholders should be planned to ensure consistent and accurate messaging from all the partner organizations.	**Payload owner Organization:** SaveForests is a small organization whose expertise is in biology and has limited resources. SaveForests does not actively manage public relations outside of business relationships. **Partner Organizations:** SatCo: SatCo's public relations do not involve SaveForests.
RC.CO-2: Reputation is repaired after an incident.	Compare post-event public relations policies/procedures to plan for after-incident response.	**Payload owner Organization:** SaveForests works with impacted parties to mitigate damage during an event and aims for an improved cyber posture after the fact. **Partner Organizations:** SatCo: SatCo's reputation repair efforts do not involve SaveForests.

CSF Subcategory	CSF Profile Applicability to HSNs	Applicability to SaveForests and Partner Organizations
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. Then, execute in a manner that is consistent with the recovery plan.	**Payload owner Organization:** SaveForests collaborates and communicates recovery and mitigation activities throughout the response plan enactment. **Partner Organizations:** SatCo: SatCo communicates recovery activities with all impacted partners.

Appendix B. Scenario Implementation Evaluation

This section is developed for the purpose of showcasing lab-based analysis and verification of operational examples listed below. These operational examples were tested in a closed lab environment as described in Sec. 3.3.1 Description of Lab Environment.

B.1. Hosted Payload Fault Example

The camera, acting as the payload, will be made to exhibit a fault code to its operation. This can be expected during operations and may be a fault in the camera system, but there could also be a cyber intrusion. The fault will be transmitted through the payload controller then through the spacecraft system to the ground computer, and it will be recorded in a database that can be shared by authorized users. The signal will be analyzed to show what fault has occurred and the normal resolution action. To understand whether the fault was caused by an equipment problem or cyber intrusion, a forensic analysis of camera data will be accomplished to understand the characteristics of anomalous events. During the analysis, the camera system will be inspected to identify any potential cyber incidents and if present, to understand attack targets and methods. Procedures will be developed to show what actions are necessary to add to normal operations anomalies for possible cyber intrusions.

B.1.1. Test Procedures

For images to be captured by the payload and viewed on the ground station, the following system process steps are performed:

1. Launch the script engine on the payload controller using the mission control software terminal or using the ground station website. The script engine is responsible for ensuring the camera power is active, initializing the SPI and secondary universal asynchronous receiver/transmitter (UART) channels, and transmitting the image capture trigger bytes over SPI to the payload to launch image capture processes onboard the camera.
2. After the image capture trigger bytes are sent by script engine 1 (SE1), script engine 2 (SE2) will be called from SE1. SE2 is responsible for receiving image bytes continuously over SPI for a fixed time until it is timely aborted by SE1.
3. Once the camera receives the appropriate trigger bytes from the payload controller for image capture, a series of onboard image processes are initialized, consisting of the following:
    a. Initializing image parameter (resolutions, frames per second (FPS), color scale).
    b. Capturing an image snapshot and converting the snapshot frame buffer data to a byte array.
    c. The byte array of X length is segmented and packaged into 32-byte segments and sent over SPI to the satellite in a for-loop until all buffer bytes are sent. The

satellite anticipates and only accepts 32-byte segments for each SPI receive command. The received 32-bytes are stored into the SE2 log file.

   d. Once all bytes are received and stored into the log file, SE2 must be aborted by SE1.

4. The ground station operator must then be able to download SE2's log file (CSP ID 32), containing the image data off the satellite payload controller.
5. Once downloaded, the log file must be post processed at the ground station level to filter out the data from the log file padding. The filtered byte array data represents a .jpeg file structure that must be saved directly as a .jpeg image file.
6. Non-corrupted .jpeg image files can then be viewed at the ground station. These steps for image capture and viewing are automated on the ground station website.

The script-engine script can monitor the state of the script engine. In case an abnormal condition occurs, an error code (fault) will be reported automatically to the ground station. An operator will check and analyze the code to determine the further actions.

B.1.2. Test Results

Faults were identified on the payload and categorized as one of five defined fault types. The five types were:

- S1.1, denoting a standard operation of the payload.
- S1.2, denoting an error offered at the initializing image capture stage of the process.
- S1.3, denoting an error occurred at the trigger to capture an image.
- S1.4, denoting an error occurred with capture of an image.
- S1.5, denoting an error occurred at the data transfer stage.

During the example test run, all success or failure logs that are generated during the image capture process are written to an internal text log file saved on board the 32 GB SD card on the camera. The logs originated from one of the four segments of the image capture process: Camera Initialization, Triggering, Image Capture, SPI image transmission. Once the script onboard the camera successfully finishes running or stops due to a fault, then the internally saved log file containing the success or failure information is processed. Then the file is transmitted over SPI with or without the image data back to the satellite payload controller where it is saved to log file 32. In the S1.2 case, where initialization fails to occur, the SPI connection cannot exist to send the image data, so a secondary UART connection is established to transmit the data. From there the log file is downloaded to the ground station where it is processed to extract the image data and the log file information.

The downloaded binary log file 32 from the satellite contains both the image data and the log data related to the fault detection information. The log data are wrapped in a unique header and end of message (EOM) to ensure that it can be parsed accurately in the end. Once the image data and logging information are parsed, the image data can be used to reconstruct the

.jpeg satellite image if image capture and transmission have no faults. The log information is saved to a unique data location on the ground station where a secondary post processing script can access the log data and upload them to a Postgre Structured Query Language (PSQL) database located on a virtual machine on the network. The purpose of this database is to allow for easy access to the log data by the ground station users, typically through the locally hosted website.

The test results show the following possible fault types from the generated log information provided by payload:

Scenario 1: Logs

S1.1 = Normal Operation

S1.2 = Initialization Fault

S1.3 = Trigger Fault

S1.4 = Capture Fault

S1.5 = Data Transmission Fault

Scenario 2: Script Change detection

S2.1 = Normal Operation, no script change detected

S2.2 = Script Modification detected

Scenario 3: Data Encryption

S3.1 = Normal operation, encryption

S3.2 = Encryption Failed

Depending on the type of log the generated, the ground station user can assess the code onboard the payload camera to identify where the issue pertains to a cyber threat or a general system malfunction.

B.2. Hosted Payload File Modification Example

A corrupted image file has been detected, and a determination needs to be made whether this is an anomaly or a cyber intrusion. The camera’s main software scripts and additional onboard supporting resources will be assessed for modifications from the original deployment and production ready scripts. The method of assessing for modifications will be done by an external security device onboard the payload platform that is connected to the camera via its micro-USB port. The external device will access the internal storage of the camera, copy, or scan the file contents, and compare the scanned scripts’ content. The comparison process would check for code syntax, character counts, or file size changes with the original ground truth reference scripts/resources that are onboard the external device. If a modification is detected, the onboard camera scripts/resources will be removed and safely stored for future assessment and an original software copy will be inserted.

B.2.3. Test Procedures

1. The external security device (ESD) hash-detecting script will be triggered prior to image capture or launched at a specific routine periodically.
2. The ESD hash-detecting script, when launched, will copy the drive image of the camera's drive and compare it to the original drive hash image stored on the ESD.
3. If the hashes differ, then the onboard camera drive contents will be transferred off the payload camera and contained on the ESD for future assessment.
4. The payload drive will then be overwritten with the original payload script contents. The ESD will be able to notify the satellite operator that a modified payload drive was detected either through notifications through the SPI channels of the payload or through direct communications on the controller area network (CAN) bus through the interface board.

B.2.4. Test Results

Once it is enabled, the security device attached to the payload can perform the security check. During the image capture process to detect if the 'main.py' (payload operation script) has been altered. The system regularly compares the file to the stored "golden copy" (file known to be correct) of the file on the security device. If the file has changed, a security program installed in the security device flags and reports the issue. The modified file is then quarantined for later evaluation. The quarantined file is removed from use and replaced by the ground truth version of the file. The payload then generates a file describing the error to be stored for reference, and the payload is rebooted to return to normal operation.

B.3. Hosted Payload Encryption Example

The camera is considered a hosted payload and is transmitting data over the satellite system to the ground system. Even if the satellite communications are encrypted, the data can be seen by other operators of the satellite. To ensure confidentiality of data, the camera can encrypt data and transfer it such that only the payload end users can view the data. The camera payload would capture an image and then the image will be encrypted using on-board capabilities. The camera would then send only the encrypted image through the payload controller and back down normal communications paths to the ground station. This would allow for a payload to fully encrypt any of the data that are transmitted outside of the payload. No part of other payloads, the satellite subsystem architecture, or ground stations would be able to monitor or view the data before they are delivered to the data owner.

Digital photo data captured by the camera hosted in the satellite are encrypted and later decrypted to demonstrate the feasibility of encrypting camera images for further transmission within the satellite systems.

B.3.1. Test Procedures

The Advanced Encryption Standard (AES) algorithm is supported on the camera and supported by the python Cryptolib module. MicroPython can import and run this module.

1. Initialize camera, take a picture, place in internal memory
2. Take a picture but don't save it to disk
3. Generate initialization vector (IV)
4. Encrypt the image using AES-256 (and the IV)
5. Save the ciphertext (encrypted image)
6. Send the ciphertext

B.3.2. Test Results

The payload can encrypt and process the captured image data with AES 256 encryption algorithm. After creation of an image, a key was generated. When the camera divided the image into byte packets to be transferred, the generated key was combined to encrypt the data. The encrypted image data are then transmitted to the ground station and the end user through the ground station. With the correct encryption key, the end user can unencrypt the image data and view the original image. Tests also demonstrated that without a correct key or without a key, the image would not be able to be viewed if captured in transit.