Recommendations to Space System Operators for Improving Cybersecurity

Publication: April 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

I. INTRODUCTION

As space becomes increasingly integrated into daily life, from national security to finance, education, and communications, it is critical that cybersecurity is a primary consideration for owners, operators, users, and manufacturers of space-based assets. Adversaries can access vulnerabilities within connected space systems to degrade our critical infrastructure and place our nation at risk. The Space Systems Critical Infrastructure Working Group (SSCIWG) is tasked with helping the space systems community improve their cybersecurity and their resilience to cyberattacks. The SSCIWG was created in compliance with the Critical Infrastructure Partnership Advisory Council (CIPAC) to enable the members to deliberate and achieve consensus advice to the federal government. This document outlines some of the most common sources of cyber risk to space systems and provides mitigation options aligned with the National Institute of Standards and Technology's (NIST) guidance and recommendations. The SSCIWG recommends for this document to be used in conjunction with the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to inform the development of cybersecurity framework profiles (CFPs), risk mitigation plans, and cybersecurity strategies. Accordingly, this report is focused on issues and concerns specific to the commercial space ecosystem. The findings of this white paper, found below, represent the thoughts and recommendations developed by public and private sector members of the SSCIWG.

The SSCIWG urges all entities who manufacture, own, operate, or use space-based assets and capabilities–whether civilian, U.S. government, intelligence, defense, or commercial–to incorporate the recommendations in this report. Doing so will support a stronger defense response to the cyber risks of space-based systems. Successful implementation will require a whole-of-government approach, as well as collaboration across manufacturers, vendors, and operators of the technology used in space systems.

II. BACKGROUND

It is an exciting time in the space industry. Thanks to recent technological innovations and decreasing cost, space is more accessible than ever, resulting in rapid advancements in communications, space tourism, mining, and more. Government and industrial activity in the U.S. are heavily reliant upon space services for operations such as geolocation, tracking, and communications capabilities. However, as space-based services become an integral part of daily life, cyber criminals and other threat actors will attempt to find new attack surfaces in space assets to further their own monetary or geopolitical gains.

A. NIST CYBERSECURITY FRAMEWORK (CSF) AND IMPACT ON SPACE ASSETS

The U.S. government provides resources to commercial operators of critical infrastructure to use to improve cybersecurity and reduce risk. The NIST Cybersecurity Framework (CSF) is one such tool that critical infrastructure operators, including those that manufacture and operate space systems, can use to better understand proven strategies for reducing cyber risk. As stated in the CSF:

> ...the Cybersecurity Enhancement Act of 2014 (CEA)[1] updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them

[1] S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act of 2014. *Congress.gov*, Library of Congress, December 18, 2014, https://www.congress.gov/bill/113th-congress/senate-bill/1353. Accessed on June 30, 2023.

identify, assess, and manage cyber risks."[2] This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution.[3]

The NIST CSF is a non-regulatory, voluntary tool that can be tailored to the specific needs of users. The CSF provides a guide on how to apply the security and privacy controls for information systems and organizations (outlined in NIST 800-53)[4] in a flexible manner based on organizational risk and business needs through the creation of a CFP. This document can assist space system manufacturers and operators with laying a foundation for the development of a CFP by understanding and prioritizing cyber risk to their systems and identifying mitigation actions. This broader understanding can then inform the development of a CFP by aligning NIST CSF Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization and will help to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals.

III. CYBER CHALLENGES TO SPACE SYSTEMS

A. UNIQUE CHARACTERISTICS OF SPACE SYSTEMS

With the development of new and increased use of space resources, cybersecurity professionals are seeing threats and vulnerabilities that are not necessarily present in terrestrial operations or may be observed in a different manner with different impacts. Space operations have distinctive characteristics, which require a unique approach to ensure safe and secure operations in a continually evolving environment. Additionally, space cybersecurity is driven by cybersecurity concerns that are not present for most terrestrial operations, including:

1. Space is a shared, common resource that can be accessed globally by governments and private-sector organizations.
2. Due to high costs and considerable deployment times, space-based network designs may struggle to keep pace with evolving cybersecurity threats. As such, the cyber mitigations built into some space systems may be obsolete before or shortly after the systems are launched.
3. A significant amount of the space network resides in space and the physical architecture of the systems must be designed to last for the life of the asset once in orbit. Since space-based assets often last a decade or longer, upgrading the architecture could be difficult or impossible, leaving the asset vulnerable to cyberattacks. In addition, there can be on-board hardware and physical failures over time that cannot be addressed fully, if at all.
4. Due to the high cost of development and delivery and the need to ensure compatibility with the greatest number of customer requirements, many operators are unable to harden key portions of the network, employ encryption in their communications on a transmit, receive, or transmit/receive basis, or incorporate on-board monitoring into space system designs.
5. Small space systems, which are built using commercial-off-the-shelf technology and components, lack integrated cybersecurity capabilities. This is done for various reasons including budget constraints,

[2] S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act of 2014, *Congress.gov*, Library of Congress, December 18, 2014, SEC.101. Public-Private Collaboration on Cybersecurity, (b)(iii) https://www.congress.gov/bill/113th-congress/senate-bill/1353. Accessed on June 30, 2023.
[3] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov), National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed on June 30, 2023.
[4] National Institute for Standards and Technology Special Publication (NIST SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020 (includes updates as of December 10, 2020), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Accessed on June 30, 2023.

lack of properly trained individuals to incorporate communications and information security into the platform, and time constraints.

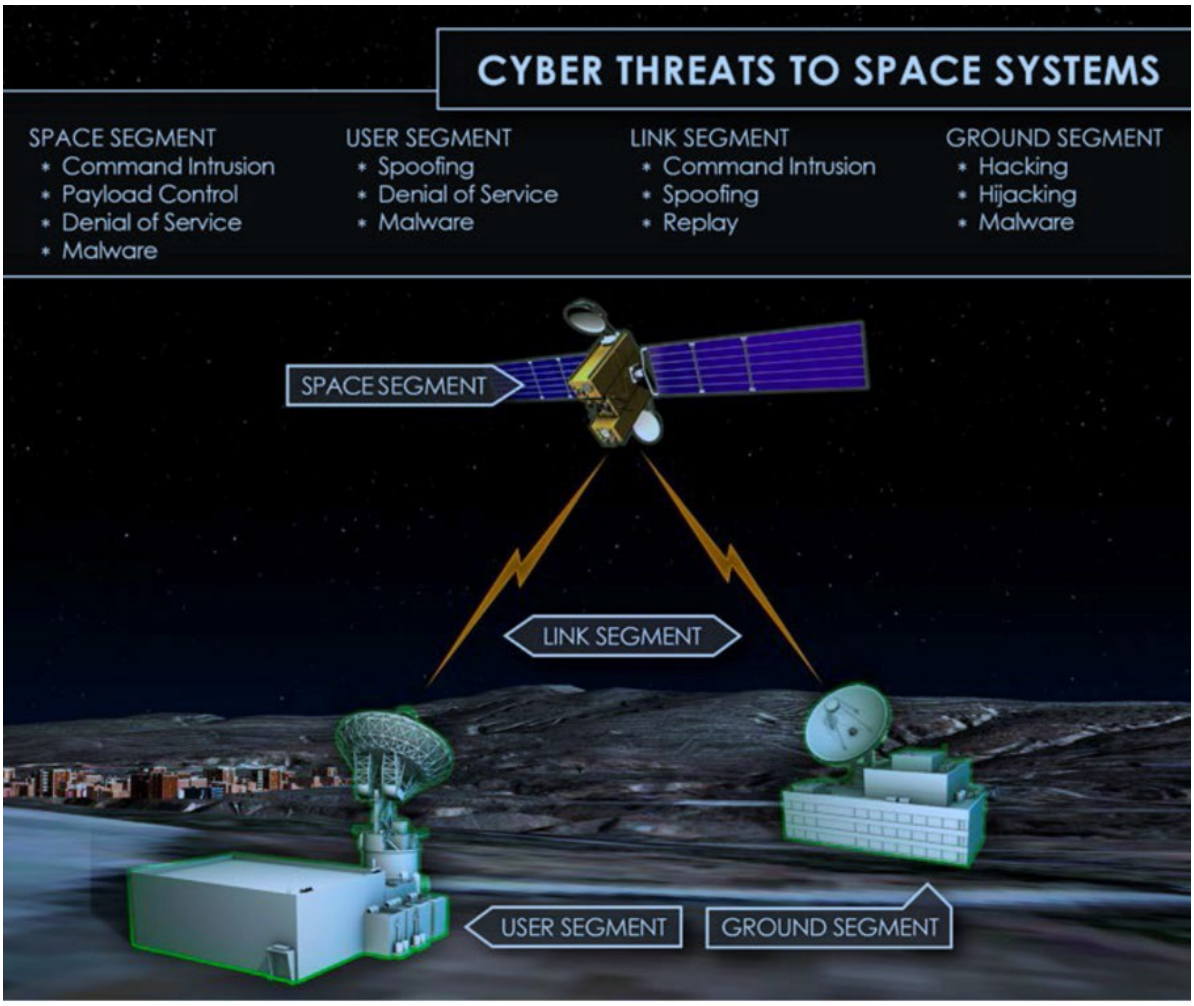
B. COMPOSITION OF SPACE SYSTEMS

Space systems are comprised of four primary segments: Space, Ground, Link, and User segments.[5] They each play a unique role in the operation and function of space assets. These segments have numerous potential risks, including threats that originate in other network segments and cascade to others. *Figure 1: Cyber Threats to Space Systems* highlights some of the specific threats below. Understanding the threats between all segments is important to understanding the risks associated with space systems and the intricacies of the segments as a whole.[6]

[5] National Air and Space Intelligence Center (NASIC), "Competing in Space," December 2018. https://www.nasic.af.mil/Portals/19/documents/Space_Glossy_FINAL--15Jan_Single_Page.pdf?ver=2019-01-23-150035-697. Accessed on June 30, 2023.

[6] National Air and Space Intelligence Center (NASIC) and Defense Intelligence Agency (DIA) have published papers on the topic of cyber threats to space systems. The risks are grouped with the various segments of space systems (Ground, Link, User, Space).

Figure 1: Cyber Threats to Space Systems[7]



C. SPACE SEGMENT RISK

Space segment assets are unique in that they are mostly inaccessible after launch and are limited to the communications technology installed during the initial construction of the assets.[8] Because space segment assets have traditionally relied on command-based communications from the ground segment, opportunities for a direct attack against the space segment asset, without going through the ground segment systems, have been limited. As such, dated technologies and a lack of necessity at the time of engineering resulted in many assets designed without communications security protection built into their internal systems or intended to be a part of its life cycle. Securing ground segment technologies and infrastructure has traditionally been, and remains, one of the most effective ways to protect assets in space.

---

[7] National Air and Space Intelligence Center (NASIC), "Competing in Space," December 2018. https://www.nasic.af.mil/Portals/19/documents/Space_Glossy_FINAL--15Jan_Single_Page.pdf?ver=2019-01-23-150035-697. Accessed on June 30, 2023.

[8] In the coming years, options for in-orbit servicing (IoS) of space assets are expected to become more available, especially as more manufacturers adopt safety and hardware standards. In 2021, Northrop Grumman demonstrated a proof of concept for IoS when it launched its first Mission Extension Vehicles, which provide station-keeping services for geostationary satellites that were running low on fuel.

Evolving technologies and requirements have allowed new space assets to use cyber-enabled technology for daily operations and functions. However, many legacy space segment assets, and even some new systems, do not include cyber-enabled technologies in their construction. As space segment assets begin to include new methods of communication, the attack surface for these devices increases and integrating new cybersecurity protections becomes increasingly necessary. Tools such as the NIST CSF can be used to build a risk profile for space segment assets to better understand and mitigate these risks. An example of how the CSF can be applied to the Space Segment can be found in NISTIR 8270.[9]

Table 1: Space Segment Risks, and the following section of this report, outline some of the various threats and recommended mitigations to address these evolving cybersecurity issues within the space segment and can be used to inform the development of a CFP.

Table 1: Space Segment Risks

Threat	Description	Mitigation
Command Intrusion/Payload Control	Establishing an unauthorized link to a space system and manipulating the system to ingest and execute malicious commands, just as it would process a legitimate set	• Deploy network segmentation and segmentation principles • Develop robust supply chain security plans and programs • Employ strong encryption (where possible)
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system	• Implement network security governance policies • Employ the concept of least functionality • Ensure supply chain vendors are employing proper cybersecurity measures • Test products/software before introducing them to a network

Command Intrusion/Payload Control

Threat

As with the ground segment, a command intrusion could allow an attacker to establish an unauthorized link to a space system and manipulate it to ingest and execute malicious commands. The command intrusion could potentially direct the space system to enter safe mode, maneuver into the path of another space system, or deorbit. These types of scenarios could result in destructive outcomes such as communications degradation or blackouts. The space system operators may be unaware of the command intrusion if the space system is not in view of a telemetry site that would provide an indication of a change. Additionally, many space systems contain multiple payloads to perform various missions, communications, and tasks for their operators. The multiple payload infrastructure and communication paths can create additional routes for attackers to gain access to a system and manipulate the payload control or cause damage to the asset.

[9] Scholl, Matthew, Theresa Suloway, "*Introduction to Cybersecurity for Commercial Satellite Operations,*" National Institute of Standards and Technology, Draft (2nd) NISTIR 8270, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf. Accessed on June 30, 2023.

Recommended Mitigation

Due to the increasing complex designs of space platforms using new technology, protection of payloads is important to the cyber resilience of the platform. Modern deployments of space systems should ensure integrity of critical operational networks remains intact by deploying network segregation and segmentation principles (NIST 800-53 Rev 5 AC-4, AC-10, SC-7), as well as developing a robust supply chain security plan or program that emphasizes maintaining valid sources of space system components and associated data (NIST 800-53 Rev 5 SR-2, SR-3, SR-4). Additionally, where possible, a strong encryption and authorization program on board the spacecraft will enable it to refuse unauthorized commands.

Malware

Threat

Malware, or software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system, is just as much of a threat to space systems as it is to other critical infrastructure systems. Gaining unauthorized remote access into Earth-based networks and installing malware can result in operational disruption of any targeted component on board the spacecraft.

Recommended Mitigation

Employing good governance practices, such as those that control access to sensitive systems, limit privileges, and securely authenticate users can help reduce exposure to malware. Similarly, technical measures such as firewalls and antivirus software reduce the risk of malware delivery to space platforms. Operators can prevent unauthorized commands (e.g., out-of-bounds commands, unhandled commands) from accessing and delivering malware to the system by employing the concept of least functionality (NIST 800-53 Rev 5 CM-7) to ensure that engineering systems respond to requests and executables in a predictable and secure manner. Additionally, having a secure software supply chain that includes defining cybersecurity expectations for vendors in contracts and testing all software and hardware before introducing it to a system can prevent the introduction of unexpected malware or vulnerabilities.

D. GROUND SEGMENT RISK

The ground segment is the most accessible and vulnerable part of the space infrastructure to cyberattacks. The ground segment may consist of multiple antenna locations and intertwined business information technology (IT) and space mission IT systems, as well as industrial control system (ICS), cloud, and other network-based services. Because ground segments are typically the most interconnected and vulnerable points in a space system, many cyberattacks originate there. An example of how to apply the NIST CSF to the ground segment can be found in NISTIR 8401.[10] Subsequently, many of the cybersecurity threats associated with space system ground segments mirror those with terrestrial counterparts, and many of the mitigation measures are the same.

The various threats and recommended mitigations to address these evolving cybersecurity issues within the ground segment are outlined in *Table 2: Ground Segment Risks* and discussed in detail in the following section.

[10] Lightman, Suzanne, et al. "Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control," Initial Public Draft NSITIR 8401, https://csrc.nist.gov/pubs/ir/8401/final. Accessed on July 27, 2023.

Table 2: Ground Segment Risks

Threat	Description	Mitigation
Hacking and Hijacking	Gaining unauthorized access to data in a system or computer and preventing the legitimate controllers from accessing the space system	• Develop strong network security governance policies • Employ technical capabilities to prevent unauthorized access and network activity • Implement protections and controls in the design, operation, and maintenance of systems • Adhere to defense-in-depth principles • Emphasize supply chain risk management • Employ strong encryption (where possible) • Use an Intrusion Detection System (IDS)
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system	• Ensure networks and hardware are using the latest software and firmware updates • Employ incident monitoring, event logging, vulnerability assessments, and continuous monitoring • Employ automated tools to assist in awareness, detection, and accuracy of monitoring information

Hacking and Hijacking

Threat

Hacking involves gaining unauthorized access to data in a system or computer, while hijacking is a method an attacker uses to prevent the legitimate controllers from accessing the space system. After access has been attained through a successful hack, an attacker targeting a space system will attempt to gain access to the command-and-control software of the system. Upon acquiring access, the attacker can control its behavior and communications by sending commands to the space system. An encrypted link between the ground and space system does not help in this scenario, as the attacker can now carry out the attack using the system's legitimate encryption infrastructure. An attacker may choose to embed their malicious commands into an otherwise legitimate command set or may hijack the system altogether. Additionally, attackers can use emerging threats to the supply chain for information and communication technology (ICT) components to obtain unauthorized access to space systems. Attackers can use advancements of commercially available space system technology and components to compromise a supply chain and introduce vulnerabilities into software or hardware that enable unauthorized access to sensitive systems.

Recommended Mitigation

Operators should have governance policies in place at the ground segment level, with technical capabilities to prevent unauthorized access and network activity. Adhering to principles of defense-in-depth, as outlined in the NIST CSF and The Aerospace Corporation's *Center for Space Policy and Strategy: Defending Spacecraft in the*

Cyber Domain,[11] will significantly reduce the risk of an intrusion. Owners and operators should ensure that appropriate protections and controls are implemented in the design, operation, and maintenance (e.g., patches, upgrades) of ground segments and design systems with multiple layers of defense including technical capabilities such as an Intrusion Detection System (IDS). Using an IDS at the ground segment could prevent hijacking by identifying unauthorized maneuvers, malicious commands, or other anomalous behaviors, and by alerting ground operators before the spacecraft is in view of a downlink site.

Supply chain threat mitigation can include activities such as: requiring a software and/or hardware bill of materials to verify a product is secure; performing security, environmental, and functionality tests on the product prior to deployment; and requiring self-attestation of cybersecurity hygiene from vendors or suppliers evaluating the product.

Malware

Threat

As in all the other segments of the space system, malware is a key threat. Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. An attacker can embed malicious software that is sent to a space network to gain access to, or damage, the system. Like their terrestrial counterparts, space systems occasionally require software updates to maintain security and improve functionality. Downloading and installing a legitimate patch, without following proper security measures, can inadvertently provide an attacker with the means to deliver malware to the space system.

Recommended Mitigation

Ground segment networks should update space system networks and hardware with the latest software and firmware updates, while simultaneously employing strong software supply chain and testing protocols. Additionally, operators should follow the recommendations outlined in the NIST CSF, with a particular emphasis on the Detection and Response functions. Specific activities that operators should employ include incident monitoring (NIST 800-53 Rev 5 IR-5), event logging (NIST 800-53 Rev 5 AU-2), control assessments for vulnerability tests (NIST 800-53 Rev 5 CA-2), continuous monitoring (NIST 800- 53 Rev 5 CA-7), and, where possible, employ automated tools to assist in awareness, detection, and accuracy of monitoring information.

E. UPLINK AND DOWNLINK SEGMENT RISK

While there are numerous threats to the uplink/downlink between the spacecraft and the ground, link segment attacks typically require specialized equipment (e.g., separate antenna). Additionally, that equipment must be targeted directly at the receiver, which limits the ability of a malicious actor to attack. For example, to successfully attack a space system in low-earth orbit, ground equipment must be precisely in line with the space system at the right moment during the flyover.

Some threats and recommended mitigations to address cybersecurity challenges to the uplink and downlink segments are outlined in *Table 3: Uplink and Downlink Segment* and discussed in detail in the following section. Threats to the link segment often involve the compromise of the ground segment (e.g., hacking,

[11] Bailey, Brandon, et al. "*Defending Spacecraft in the Cyber Domain,*" The Aerospace Corporation, Center For Space Policy and Strategy, November 2019, https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf. Accessed on June 30, 2023.

malware) or impacts to the space segment (e.g., command intrusion). These threats are detailed in previous sections and will not be addressed in this section.

Table 3: Uplink and Downlink Segment

Threat	Description	Mitigation
Jamming and Spoofing	Denying the ability of the legitimate command and control to deliver commands and disguising a communication from an unknown source as originating from a known, trusted source	• Employ hardware-based solutions such as controlled reception pattern antennae (CRPA) • Use encrypted communication and ground segment-based protection measures, where possible, to mitigate and prevent unauthorized communication with space platforms and traffic scanning
Replay	Recording a previous command sent to the space system and playing it again later	• Employ strong encryption, where possible

Jamming and Spoofing

Threat

Space systems are inherently dependent on wireless and radio communications within the electromagnetic spectrum. These communications can be jammed in multiple ways including using the electromagnetic spectrum to produce noise that prevents the receiver from accessing legitimate signals or by compromising the stream of data to a receiver, which denies the ability of the legitimate command and control to deliver commands. Spoofing is the act of disguising a communication from an unknown source as originating from a known, trusted source. Spoofing may be executed in conjunction with the jamming of a legitimate set of commands. Because spoofing is intended to look like a transmission from a legitimate source, the spoofed command may be transmitted close to an authorized ground station.

Recommended Mitigation

Standard RF-spectrum protections for telemetry, tracking, and command systems (TT&C), including hardware-based solutions such as controlled reception pattern antennae (CRPA), have been successfully demonstrated by the U.S. military (and others) to reduce the impacts of jamming and spoofing for lower RF band frequencies. Additionally, space system operators should use encrypted communication and ground segment-based protection measures, where possible, to mitigate and prevent unauthorized communication with space platforms and traffic scanning.

Replay

Threat

Replay is when an attacker records a previous command sent to the space system and replays the command set at a later time. This allows the attacker to use the legitimate command structure and encryption, thus gaining the capability to access the space system. The attacker cannot change the content of the message but can make the space system execute the command at the time of their choosing.

Recommended Mitigation

Replay attacks have a better chance of mitigation with a strong encryption program as they involve the use of a separate set of antenna equipment and ground infrastructure to carry out an attack. This is in contrast with the previous ground segment attacks, which use equipment native to the space system.

F. USER SEGMENT AND USER DEVICES RISK

There are many different types of users for space systems, which include communications, sensory applications, and space travel, as well as Position, Navigation, and Timing (PNT). The user segment is defined by entities located on the surface of the Earth, which are transmitting and receiving signals from the space system. Many intrusions from cyber occur at the user level since many users do not view the terminal to be as vulnerable as their other communications networks and, subsequently, do not take appropriate cyber precautions. Risk to terminals varies depending on the type of device that is in operation. For instance, GPS end users only receive signals from the space system (passive reception), indicating their exact position on Earth. Whereas other assets, such as satellite phones, contain a transmission and receiving capability. To illustrate the attacks on the user segment, consider using NISTIR 8323.

User segments often require regular updates and patches, much like other components of space systems. As with ground systems, malware is a threat to any asset that has access to the internet, or to an internet-connected device. However, the recommended mitigations for avoiding malware in a user segment do not significantly differ from the recommendations listed previously under the ground segment. Some additional threats and recommended mitigations to address cybersecurity challenges to the user segments are outlined in *Table 4: User Segment Risk* and discussed in detail in the following section.

Table 4: User Segment Risk

Threat	Description	Mitigation
Spoofing	Disguising a communication from an unknown source as originating from a known, trusted source	• Employ hardware-based solutions such as GPS receivers that null signals received from a ground-based source • Use encrypted communication, where possible, to prevent unauthorized communication with space platforms and traffic scanning
Denial of Service	Broad-based noise or a set of data, which is repeated in such a way as to prevent the receiver from executing proper internal functions	• Employ strong encryption, where possible • Employ hardware-based solutions such as specialized antennas

Spoofing

Threat

Spoofing is a potential attack vector for all user terminals. In a spoofing attack, malicious actors will attempt to deceive a user terminal by sending an unauthorized signal that is masquerading as a legitimate signal from a

space system. Additionally, the malicious actor may attempt to spoof a signal from a legitimate space system, such as a satellite, to a ground emitter. For example, spoofing the space-based internet signals is a way to introduce malware into a user's computer.

Recommended Mitigation

NISTIR 8323 informs users of satellite-based PNT to ensure the signals they are receiving are coming from a source above the horizon. Currently, there are GPS receivers that will null GPS signals coming from a ground source. Additionally, the use of encrypted communication between space segments and user segments, where possible, can help to mitigate the risk of unauthorized communication with space platforms and traffic scanning.

Denial of Service

Threat

Denial of service for the user segment could derive from various sources and take on the form of broad-based noise or a set of data, which is repeated in such a way as to prevent the receiver from executing proper internal functions.

Recommended Mitigation

Encrypted communication and ground segment-based protection measures, such as specialized antennas, can mitigate and prevent unauthorized communication with space platforms and traffic scanning.

IV. CONCLUSION

As outlined above, much of the cyber risk to space systems closely mirrors risk to terrestrial systems and space system stakeholders can mitigate risk in similar ways. The most important thing when considering cyber risk is the unique environment and characteristics inherent in space systems. Space systems suffer from a number of challenges that are more pronounced than most terrestrial systems, including Size, Weight, Power, and Cost (SWPAC), which can limit the security capabilities of the space system. All factors should be taken into consideration when conducting a cyber risk assessment and should be used to inform the development of a CFP that can be tailored to the specific needs of the users, manufacturers, owners, and operators. Space system stakeholders should use the common cyber risks outlined in this report to inform their profile and carefully analyze the risks for each segment of their space system including:

- Implement protections and controls in the design, operation, and maintenance of systems including adhering to defense-in-depth principles and deploying network segmentation and segmentation principles.
- Emphasize supply chain risk management by developing and employing supply chain security plans and programs, ensuring vendors are employing proper cybersecurity measures, and testing products/software before introducing them to a network.
- Employing technical capabilities to prevent and detect unauthorized access and network activity such as automated tools to assist in awareness, detection, and accuracy of monitoring information, strong encryption (where possible), and hardware-based solutions that limit adversaries' abilities to spoof or jam signals.

- Develop and implement strong network security governance policies that require (where possible) incident monitoring, event logging and review, vulnerability assessments, continuous monitoring, and updating all networks and hardware to the latest software and firmware.

By increasing awareness of cyber threats and the measures available to prevent or mitigate their impacts, owners, operators, users, and manufacturers of space systems can significantly reduce the likelihood of an incident that will threaten the reliability of their space system. As critical infrastructure increasingly relies on space systems as a foundation for reliable operations, it is critical that space systems keep pace with and, where possible, exceed the capabilities of malicious cyber actors to safeguard the security of our economy, public health, and the nation.

APPENDIX A: WORKING GROUP MEMBERS

Member	Company/Agency
Geoffrey Bull	National Geospatial-Intelligence Agency
Edna Conway	Microsoft
Trevor Garner	National Geospatial-Intelligence Agency
Ashley Gerwitz	Cybersecurity and Infrastructure Security Agency
Lori Gordon	The Aerospace Corporation
David Logsdon	CompTIA
Jennifer Manner	EchoStar/Hughes
Jenny Margaros	Cybersecurity and Infrastructure Security Agency
Erin Miller	Space Information Sharing and Analysis Center
John Ransom	Cybersecurity and Infrastructure Security Agency
Daniel Roccaforte	Maxar
MJ Shoer	CompTIA
Theresa Suloway	MITRE
Lucas Truax	Stephenson Stellar
Ernest Wong	Department of Homeland Security

APPENDIX B: ACRONYMS

Acronym	Full Name
AST	Office of Commercial Space Transportation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSP	Committee on National Security Systems Publication
CRSRA	Commercial Remote Sensing Regulatory Affairs
CTO	Chief Technology Officer
DOT	Department of Transportation
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FOIA	Freedom of Information Act
IR	Internal Report
ITL	Information Technology Laboratory
LEO	Low Earth Orbit
NCSPA	National and Commercial Space Programs Act
NESDIS	National Environmental Satellite, Data, and Information Service
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
OSC	Office of Space Commercialization
PPD	Presidential Policy Directive
SP	Special Publication
USG	United States Government

APPENDIX C: U.S. GOVERNMENT ACTION AND RESOURCES

SPACE POLICY DIRECTIVE–5

In 2020, the U.S. government issued *Space Policy Directive-5 (SPD-5)–Cybersecurity Principles for Space Systems (SPD-5)*[12] in response to evolving cyber threats to space systems. This directive instructs U.S. federal departments and agencies to, "…foster practices within Government space operations and across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations."[13] The mandate applies existing cybersecurity strategies currently in use in terrestrial systems to space systems and asks space system operators to enhance their cyber preparedness by developing systems that can, "…continuously monitor, anticipate, and adapt to mitigate evolving malicious cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations."[14] To accomplish this, SPD-5 outlines a series of activities, including improvements to cybersecurity planning and hygiene, enhancing physical and logical access controls, securing supply chains, and protecting against jamming and spoofing.[15] These activities are intended to reinforce the need for enhanced cyber-preparedness with the goal of protecting the security, economic prosperity, and scientific knowledge of the U.S.

One application of SPD-5 was in response to Russian cyber activity in the Ukraine/Russia conflict targeting satellite communications (ViaSat commercial and by extension as a defense contractor in that region). In this instance, the U.S. National Security Agency (NSA) released a Cybersecurity Advisory (CSA) in May 2022, titled *Protecting VSAT Communications*. The advisory built upon SPD-5 by calling on space system operators to secure very small aperture terminal (VSAT) networks through various technical means to include encryption. Additionally, the advisory aimed to help organizations understand how communications may be at risk of compromise and how they can act to reduce risk.

FOUNDATIONAL PNT PROFILE: APPLYING THE CYBERSECURITY FRAMEWORK FOR THE RESPONSIBLE USE OF POSITIONING, NAVIGATION, AND TIMING (PNT) SERVICES (NIST IR 8323)

The national and economic security of the U.S. depends on the reliable functioning of Positioning, Navigation, and Timing (PNT) services. In a U.S. government-wide effort to mitigate the potential impacts of a PNT disruption or manipulation, *Executive Order (EO) 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation and Timing Services* was issued on February 12, 2020. Section 4 of EO 13905 directs the Secretary of Commerce, in coordination with the heads of Sector-Specific Agencies, to develop PNT profiles to manage risks to the systems dependent on PNT services. NIST produced a PNT foundational cybersecurity profile, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (NIST IR 8323)*, in response to Section

[12] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House (archives.gov), https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/. Accessed on July 27, 2023.
[13] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House (archives.gov), Sec. 3. Policy, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/. Accessed on July 27, 2023.
[14] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House (archives.gov), Sec. 4. Principles, (a), https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/. Accessed on July 27, 2023.
[15] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House (archives.gov), Sec. 4. Principles, (b)(i-vi), https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/. Accessed on July 27, 2023.

4 of this Executive Order. The PNT Profile was created by applying the widely used NIST Cybersecurity Framework and is used as part of a risk management program to help organizations manage risks to systems, networks, and assets that use PNT services. NIST recently announced it would update this profile, which is currently out for stakeholder review and comment.

INTRODUCTION TO CYBERSECURITY FOR COMMERCIAL SATELLITE OPERATIONS (NIST IR 8270)

The Introduction to Cybersecurity for Commercial Satellite Operations (NIST IR 8270) provides a general introduction to cybersecurity risk management for commercial satellite operations. It presents basic concepts, generates discussions, and provides sample references for additional information on pertinent cybersecurity risk management models for use by the industry as they begin to start managing cybersecurity risks to commercial satellites. In this way it is not a comprehensive cybersecurity guidance. This report was written in response to the 2018 Cybersecurity National Strategy and in support of Space Policy Directive-5—Cybersecurity Principles for Space Systems.

SATELLITE GROUND SEGMENT: APPLYING THE CYBERSECURITY FRAMEWORK (CSF) TO ASSURE SATELLITE COMMAND AND CONTROL (NIST IR 8401)

Satellite Ground Segment: Applying the Cybersecurity Framework (CSF) to Assure Satellite Command and Control (NIST IR 8401), applies the NIST Cybersecurity Framework to address the risks of the ground segment of space operations. The document defines the ground segment, outlines its responsibilities, and presents a mapping to relevant cybersecurity information references. The profile defined in this report provides a flexible framework for managing cybersecurity risk and continues to address the goals of Space Policy Directive-5 for securing space.

APPENDIX D: GLOSSARY

Term	Definition
Beacon	Initial signal by satellite conducted when first put into mission operation in order to establish communications with command and control and report initial operating status
Crosslinks	Communication between satellites
Current Profile	The "as is" state of system cybersecurity
Downlink	Communication originating from the satellite to the ground
Payload	Mission-specific items of the overall satellite that are not part of the overall operations or "flying" of the satellite
Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring
Satellite	Bus and payload combined into one operational asset
Target Profile	The desired outcome or "to be" state of cybersecurity implementation
Telemetry	The science of measuring a quantity or quantities, transmitting the results to a distant station, and interpreting, indicating, and/or recording the quantities measured
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; the potential for a threat-source to successfully exploit a particular information system vulnerability
Uplink	Communication originating from the ground to the satellite
Vehicle	Space operational items that include the launching items used to place the satellite, bus, and/or payload into orbit
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

PRODUCT SURVEY

The Cybersecurity and Infrastructure Security Agency's National Risk Management Center welcomes your feedback. Please complete the product survey at Recommendations to Space System Operators for Improving Cybersecurity, or scan the QR code below: