HOUSE SCIENCE, SPACE AND TECHNOLOGY COMMITTEE
SUBCOMMITTEE ON SPACE AND AERONAUTICS
JULY 28, 2022

WRITTEN TESTIMONY FOR DR. THERESA SULOWAY, MITRE CORPORATION

Good morning. My name is Dr. Theresa Suloway, and I am a space and cybersecurity engineer and program manager with The MITRE Corporation. I am grateful to Chairman Beyer, Ranking Member Babin, and the members of the Space and Aeronautics Subcommittee for inviting my testimony today, and appreciate the Committee's leadership on this issue and your attention to these important challenges.

My testimony today is as a subject matter expert on space cybersecurity, developed from my experience working at MITRE and my 15 years of technical experience guiding research and development and operational activities in the Defense and Intelligence Communities. I also serve as an alternate member of the Space Information Sharing Working Group, a permanent working group of the Space Information Sharing and Analysis Center, or ISAC.

My role with MITRE, a not-for-profit organization chartered to operate in the public interest, has involved leading research and development to support NIST's National Cybersecurity Federally Funded Research and Development Center (FFRDC). This FFRDC administers NIST's National Cybersecurity Center of Excellence, or NCCOE, which MITRE has operated since 2014. FFRDCs are unique organizations that assist the U.S. Government with scientific research and analysis; development and acquisition; and systems engineering and integration. MITRE operates six FFRDCs; a wide variety of labs to advance research, collaboration and innovation in technology and mission areas; and a non-profit foundation for the public good.

Both my work with NIST for MITRE, and my research inform my thinking on today's topic, cybersecurity issues for civil and commercial space systems. In my testimony today, I would like to focus on the most critical cyber risks to commercial space systems and on how exploiting them could affect these systems and their users, and provide some recommendations on ways those risks can be mitigated.

Understanding the Domain

When discussing space systems, it is helpful to break the domain into three manageable, distinct components: the user segment, the ground segment, and the space segment.

The user segment is the community that uses the services that the satellite provides. This can be a passive user, who only receives a signal, such as GPS services or remote sensing data (optical and other phenomena), or an active user, who also sends a signal to a satellite, as in the case of satellite communications (including internet services). In general, the user is not associated with the control of the satellite or its payloads.

The ground segment in this case is defined by the infrastructure that supports the tasking and operation of the satellite and its payload or payloads. This includes the computer networks as well as the antennas, antenna support equipment, and industrial control systems (ICS) that support antenna

pointing and computer operations. Because of its physical location, the ground segment is the most easily accessible to malicious influence and needs to be secured.

The space segment represents the satellite or other platform (such as a space station) that is in orbit. The satellite receives commands from the ground segment and provides services to the user segment. Each segment has unique challenges, and the following NIST Interagency Reports (NISTIRs), which I co-authored in my role with MITRE, were written to help address these needs, and cumulatively constitute NIST's Cybersecurity Framework for space:

NISTIR 8323 – Focused on the passive user of position, navigation, and timing (PNT) services
NISTIR 8270 – Focused on the space segment
NISTIR 8401 – Focused on the ground segment, and produced with support from U.S. Space Force

There is also a new Hybrid Satellite Networks publication recently released by NIST for comment which addresses the space segment, but with a specific focus on payloads, and is being developed with the financial support of the U.S. Space Force.

Key Challenges for the Commercial Space Community

The commercial space community has a unique set of cybersecurity challenges for new and existing entrants. There is a high cost of entry to set up the ground infrastructure to control a satellite, from the antennas, antenna pointing equipment, ICS systems and computer networks. There is also the cost of the land and the regulatory compliance with transmitting that can be costly and time consuming. Due to these fixed costs, many commercial companies are turning to shared services models which increase cybersecurity risks to the commercial space community.

For example, some commercial satellite companies utilize a "ground station as a service" model so they don't need to buy equipment and hire staff to support the communication to the satellite. Smaller commercial satellite companies can pay a fee for the use of a ground station service and use their resources on developing their satellite or payload. However, the risk accepted by one company may be imposed on the other tenants on the shared ground station. Each satellite operator accesses the ground station as a service as a remote user, potentially exposing controls to the internet. A satellite operator remotely accessing the ground service could unknowingly introduce a malicious set of code to the ground station, resulting in an attacker having executable privileges on the ground equipment. This executable code could allow the attacker to view commands being sent to other satellites and access the commanding infrastructure to deliver malicious commands or exploits to the satellites themselves.

Additionally, many companies in the commercial space industry are focused solely on user-facing payload development, leveraging a "satellite vehicle as a service." This model of a hosted payload, or a payload that is attached to a satellite manufactured and operated by a different company, also presents challenges from a cybersecurity perspective. A satellite architecture typically consists of a mission computer and a control communication backbone called a bus, which serves as the communication path between the mission computer and the sensors, control mechanisms and payloads. This data bus needs to operate in real time to control the satellite. While this linkage is essential for payload operation, it

also introduces potential vulnerabilities into the system by creating an avenue to attack the satellite vehicle through an unsecured payload. An example of this type of attack was demonstrated on a car several years ago. The entertainment system of the car, running a similar kind of bus, was directly connected to the car's central control computer. Attackers were able to access the entertainment systems of the car, and ultimately stop the car using the entertainment system, or "payload," as an access point to the car's central control system. A satellite hosting a payload is vulnerable to similar threats.

Commercial space companies that serve DOD customers have a more robust security policy as a result of more stringent federal regulation. Commercial space providers that don't serve DOD are more focused on cybersecurity that allows them to protect their Intellectual Property. The spacecraft receives minimal attention because the operators often assume that the spacecraft is physically isolated from malevolent attack. Commercial products for cybersecurity for the ground segment are more mature and could potentially mitigate some of these vulnerabilities in the space segment with appropriate testing and certification.

This shared and evolving nature of commercial space demonstrates the need for continued guidance from NIST, such as the NIST Cybersecurity Framework, which provides a common lexicon by which all private sector operators and manufacturers can communicate – for example, where efforts have been made to secure systems; which organization or organizations have addressed risk; and which risks need to be addressed by a given organization. Establishing this lexicon ensures that expectations and capabilities are clearly understood by all parties in the shared operating environment. If the nature of that sharing isn't clear, gaps in security may occur.

Cyber Risks to Commercial Space

One of the most urgent cybersecurity needs that must be addressed for commercial space is the possibility that one or more satellites could be hijacked to cause a collision in space. A collision between two commercial satellites or between a commercial satellite and the International Space Station or a national security asset would not only destroy the satellites involved, but the resulting debris would permanently remove that orbit or region from use by any other satellite. This risk requires preemptive, rather than reactive, action.

For example, commercial space systems have been funded by the FCC to enable broadband access for rural areas. Commercial space systems acting as a component of critical infrastructure serving rural and remote locations have the potential to create a single point of failure. In more populated areas, other terrestrial network links can be used if connectivity via space systems goes down, but critical infrastructure relying on these commercial space services, such as pipelines and electric grid infrastructure, in "hard to reach" locations is especially vulnerable to space failure due to the lack of similar backup systems.

Other transportation systems and critical infrastructure, including our nation's air traffic control system, which depend on our GPS, remote sensing, and communication systems, could be disrupted in similar ways. Even modern agriculture and the security of our nation's food supply rely on the information provided by space-based systems and would be significantly disrupted by such an attack.

The ground segment is also vulnerable to cyber-attack. It is the most easily accessible because it is connected to the terrestrial internet. The cost of entry for an attacker is lowest if they can gain access through traditional means by using the internet. More sophisticated attacks would require additional equipment such as antennas and antennae pointing equipment, which is harder to obtain and maintain. If someone wanted to attack a satellite, it is easier to use the existing infrastructure to connect with the satellite to deliver an exploit. The Viasat incident is a recent example from the war in Ukraine, where malware exploited a misconfigured network appliance at the ground segment. The attackers were then able to use lateral movement to send a malicious firmware update to the user segment. This update disabled the user terminal. This focused attack on the ground segment makes evident the need to address this segment.

Mitigating Risks

There are both near- and long-term measures that will mitigate these and other cyber risks. In the near-term, adding encrypted links to the tracking telemetry and control is the most critical. This encryption would prevent attackers from being able to view command controls and gain an understanding of the operating environment, closing off an attack vector. Another benefit from encryption is that it ensures the information received from the satellite is correct and accurate. For example, in an information-based attack, an attacker could send inaccurate data to the control station indicating that the satellite was in a spin. The controller would then try to correct the nonexistent spin, inducing one. Accurate and secure operational information is critical to safe and effective ground-based control.

In the long-term, with threats posed by the potential illicit use of quantum computing and other high-powered computing capabilities to encrypted communications, adding post-quantum crypto capabilities on the ground and space segments will be needed. This threat is the same challenge faced across government and industry when dealing with protecting sensitive and classified information. The problem here is that the spacecraft, once launched, is not accessible, limiting potential actions to remediate a threat. Instead, proactive steps need to be taken to add these capabilities to the commercial space domain.

Ultimately, spacecraft will need to incorporate autonomous security systems that leverage on-board sensors to determine their state of trust and whether commands from the ground are appropriate. Ensuring these autonomous systems can fit within the low Size Weight and Power (SWAP) environment needs to be an investment area. This concept is similar to the idea of zero trust systems but augmented with AI.

Finally, software patches are a critical mitigation tool to prevent cybersecurity attacks. Commercial space companies over time will use legacy, or previously flight qualified, systems as part of their design, to show investors that their products have “pedigree” of successful flight. However, from a cyber risk perspective, the longer a software component has been published, the more time an attacker has to identify a vulnerability in that software. That is why keeping software patched is critical. Using legacy software and hardware that has flight pedigree may expose users to more risk by using a dated system with more known vulnerabilities and associated exploits.

A Path Forward

Just as government and industry must work in tandem to secure the future of the space domain, Congress and executive agencies will need to work across jurisdictions to ensure success. Focusing on regulation alone, including potentially costly cybersecurity requirements, could place significant barriers on a still-emerging satellite community. The commercial space industry operates within the constraints of space, power, weight, and cost, and needs to serve both customers and investors. Introducing burdensome requirements into this already high-risk, high-cost environment without a full understanding of their impact could force companies to shift their operations to other nations, leaving the U.S. without a vital connection to the emerging commercial space community. It is important that we advance U.S. leadership in commercial space, positioning our nation's industry to establish rules of behavior and international norms through market share.

Based on my experiences in the space cybersecurity domain, I propose the following actions:

Incentivize adoption of best practices: The best method to foster adoption of cybersecurity best practices by the commercial space industry is through incentives, not regulation. Levying realistic and incremental requirements that focus on encryption of the tracking telemetry and control of the satellite systems between the ground and space segment is most important. If only one requirement is applied, ensure that it is encryption and encryption modules that can upgrade to Post-Quantum Algorithms. Invest in the flight qualification of cybersecurity technologies for the space segment. This will help to create a pedigree for cybersecurity products for commercial space.

Formalize and strengthen the government's relationship with the Space ISAC: The Space ISAC facilitates collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the space sector with respect to this information. The ISAC's cybersecurity framework focuses on the five tenets of identify, protect, detect, respond, and recover, all of which require robust space situational awareness. Monitoring and cyber situational awareness are important to cement as part of the fabric of commercial space, so in the future proliferated commercial space environment, the U.S. Government can quickly determine the risks associated with commercial space systems, and the exploits and attacks they are facing. The Space ISAC's Watch Center, coming on-line in Q4 of this year, could provide both the government and industry with this needed awareness. The ISAC is perfectly positioned to continue acting as a convener in forging the community-based consensus standards I've proposed here today, and Congress can incentivize industry to grow their participation.

Consider Designating Space Systems as a Critical Infrastructure Sector: Given the importance of space systems to National Critical Functions and all other critical infrastructure sectors, the unique missions that space systems support, the importance of these systems to our national and economic security, and the unique supply chain that supports space systems, I personally believe strong consideration should be given to designating space systems as a critical infrastructure sector. There are 16 existing critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on

security, national economic security, national public health or safety, or any combination thereof. In a world where communications and daily life are becoming more intertwined with space-based operations by the day, the space domain has never been more critical.

I remain committed to the success, safety, and growth of the commercial space domain through my work at MITRE and the Space ISAC, and with academia and private industry. I greatly appreciate the opportunity to come before you today to provide our insights and I look forward to your questions.