**Statement of**

**Mr. Brandon Bailey**

**Senior Project Leader – Cyber Assessments and Research Department**

**The Aerospace Corporation**

**Before the**
**Committee on Science, Space, and Technology**

**Subcommittee on Space and Aeronautics**

**U.S. House of Representatives**

**"Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial Space Systems**"

Chairman Beyer, Ranking Member Babin, and distinguished members of the Subcommittee, thank you for inviting me to join this discussion. I work within the Aerospace Corporation, a non-profit federally funded research and development center that has a purpose to be a fiduciary for the space domain and to provide objective advice to the government on all aspects of the nation's space enterprise. Within the last decade, Aerospace has been performing analysis and research on space system cybersecurity to protect against an evolving threat landscape. I've spent the majority of my 16-year career focusing on cybersecurity issues with commercial and civilian space systems.

It is a great pleasure to give testimony today in the subject domain that has constituted the majority of my career. The focus of my testimony will be to address the critical importance of space technology and the unique protections required to maintain our national security and world leadership in the space domain. Aerospace has focused on space technology with government customers for over 60 years. As we have researched, investigated, ensured, and protected space technology over this time, competition has emerged and significantly grown into significant threats to the United States leadership in the space domain.

Today I would like to cover several aspects within this testimony describing the current gaps in relation to cybersecurity of space technology.

- Critical need to protect space technology and likely need to create a dedicated space technology sector.
- The disjointed oversight and governance of cybersecurity for space technology
- The lack of binding space cyber policy for commercial space technology. Space Policy Directive 5 does exist, but it is non-binding and treated mostly as informational
- The significant gaps in technical cybersecure solutions, standards, and best practices for space technology

- Lack of cybersecurity information sharing, and research and development for space technology as many efforts within space-cyber are siloed and fragmented.
- Significant lack of security-focused, defensive capabilities on-board the satellites. There is too much existing focus on the ground segment protections to limit access to the satellite.
- There is a lack of technical focus on validating security implementations in space systems.
- Supply chain risk management continues to be a challenge especially with global supply chains of specialized equipment

The release of Space Policy Directive-5 in September 2020 and the fact we are having this hearing testifies to the importance of space technology and cybersecurity. These two domains are inextricably linked, and their successful integration is a must. According to SPD-5, "*...it is essential to protect **space systems** from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's **critical infrastructure***." SPD-5 establishes a definition for space system as "*a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service."* Furthermore, SPD-5 recognizes that space systems contribute to the operations of the nation's critical infrastructure. But what is critical infrastructure and is "space technology" a part of it?

According to Presidential Policy Directive (PPD) -21 the term "critical infrastructure" is defined by section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Leveraging that definition, it is unquestionable that there is space technology that qualify for the critical infrastructure definition. Space technology includes the Global Positioning System (GPS), remote-sensing satellites for environmental monitoring, weather satellites to protect our nation's operation, communications satellites for global connectivity, intelligence surveillance and reconnaissance for national security, and the launch capabilities that have enabled proliferated space systems unprecedented in the history of the world. Space technology is important for industry and government activity, as well as everyday people activities. From agriculture to national security, environmental monitoring to finance, commercial fishing to emergency services, space-based services—invisible but invaluable—enable or assist a diversity of everyday applications in ways that we may take for granted. In fact, according to DHS, all 55 of the national critical functions (NCFs) have some sort of dependency or enabled by space technology.

So, this begs the question, if space technology is so critical why is it not an officially recognized by DHS as one of the critical infrastructure sectors? That is an open topic of debate within the space community as we speak. My professional opinion is that if you leverage the definition outlined in PPD-21 then space technology is indeed critical as a sector. There are numerous assets, systems, and networks (i.e., space technology) that are vital to the United States and their incapacitation or destruction would have a debilitating effect on national and economic security.

A counter argument would be why not include the applicable space systems in their respective sectors like the communication sector or the information technology sector. While this is a possible solution, it is important to understand what occurs when a sector is deemed critical. First it would stimulate policy and stakeholder attention and resources needed to secure the space systems that support the NCFs which is a current gap for the United States. Additionally, a critical infrastructure sector designation, would be a powerful statement to adversaries that the United States intends to defend and strengthen its access to space by coupling the security of our space systems to our national and economic security. It would also serve as a "forcing function" for the government to organize its space protection efforts and elevate the visibility of space technology to industry and our international partners. Ultimately, the specific designation of space technology as sector would provide the appropriate consolidation and protection that is unique to the space domain. Without this designation, space technology will be diluted and subordinate to the other sector specific protection. Without a critical mass of focus on space technology, there is not likely sufficient focus to protect the critical space-based capabilities.

With the "why" being established, the "how" for space technology protection is the next key question to be asked. Simply stating thou shall be a critical sector without proper planning on implementation could ultimately lead to creating unnecessary bureaucracy that could stifle the innovation that is necessary to ensure the United States remains the leader in space-based capabilities along with it being secure. The space technology sector encompasses many specialized computational components that provide unique capabilities from orbit, must contend with the harsh environmental conditions of space, and accommodate strict size, weight, and power constraints for operating in space. Therefore, ensuring a proper Sector-Specific Agency (SSA), also known more recently as a Sector Risk Management Agency (SRMA), is selected along with support from other applicable Federal departments, agencies, and entities like the Space Information Sharing and Analysis Center (ISAC) who understand cybersecurity in addition to the space environment will be crucial to the successful implementation of identifying space technology as a critical infrastructure sector. The term "Sector-Specific Agency" means the Federal department or agency designated under directive PPD-21 to be responsible for providing **institutional knowledge** and **specialized expertise** as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. Aerospace has and continues to perform many of these roles. To be successful, entities involved with oversight and governance must contain or leverage entities that contain space-based institutional knowledge, expertise, and lessons learned for securing space systems. There are equipped agencies within the federal sector who have dealt with securing space assets for many years as well as entities like the Aerospace Corporation and the Space ISAC who have taken a leadership role in understanding the cybersecurity threat landscape for space and helping establish best practices in mitigating cyber risk for space systems. Leveraging the appropriate federal agencies and entities who are already working space-cyber issues, we can create a national community of stakeholders for the security and resilience of space technology, bringing public and private sectors together with a shared purpose. This national security community focused on space technology can invigorate the development of security requirements and define more effective security governance.

Since it has been established that space systems provide critical capabilities and it has been openly communicated by the Defense Intelligence Agency (DIA) that adversarial nations plan to

target the United States' space technology, it is important we understand the types of attacks the United States could encounter. Space systems face many types of attack, including orbital, kinetic, and electronic warfare, but there are also multiple forms of cyber threat. Cyber-attacks can occur across space system architecture aspects — space, communications link, ground, and launch. These architecture aspects are often overlooked in wider discussions of cyber threats to critical infrastructure. During a conflict, adversaries will seek to disrupt, deny, degrade, deceive, or destroy space capabilities.

Cyber-attacks are a complex but effective and increasingly prevalent attack vector against space technology. With the rapid commercialization of space-based capabilities, government owned assets are no longer the only space systems being targeted by adversaries. As was witnessed during the Russia-Ukraine conflict, cyber-attacks have no boundaries and commercial entities will be targeted as well. The attack on Viasat's space architecture was successful in degrading communication capabilities during the initial stages of the conflict. Security considerations and solutions must be established as the United States continues to leverage commercial capabilities to augment or replace traditionally provided government space-based capabilities. The United States cannot "hope for the best" when it comes to security on commercial space systems; action is needed to ensure commercial space systems have been built securely using threat-informed, risk-based engineering. It is also imperative that these security principles are flowed down appropriately through subsidiaries in the supply chain.

The range of possible attacks can make understanding cyber-attacks on space systems a daunting proposition. Further complicating the matter is that space systems themselves can vary greatly in both function and implementation. Threat goals impact how, when, and for what purpose hostile actors might attack a target. For instance, destroying a commercial communication satellite with a cyber-attack may be done to deny critical command and control during a conflict. Alternatively, a developing nation may seek to compromise a contractor development system to steal knowledge and intellectual property to advance their space capabilities. This is where performing threat modeling against a space-based capability is imperative. Understanding the mindset of an adversary and how they could potentially attack the space systems will ultimately help inform design decision and reducing cyber risk to the space system.

A sample list of attacks that could compromise a space system include:

- Subversion of ground system capabilities by utilizing the ground system to maliciously interact with a satellite
- Communications hacking on commanding sub-systems via command link injection, replay attacks, or electronic attacks like jamming and spoofing
- Malicious features embedded during software and hardware development. Supply chain risk management is critical and must be performed through the lifecycle across critical entities and components of the space system
- Design vulnerability exploitation, where designed-in features of the system are used for malicious purposes. Many vulnerabilities within space systems are design flaws that enable adversaries the ability to carry out their objectives.
- Software weaknesses and vulnerabilities exploitation on the ground or the satellite (e.g., poor coding practices)

- Insider threats where authorized users either maliciously or unwittingly enable attacks on the space system

With the overall advancement of knowledge around space technologies, “security by obscurity” for space systems no longer exists, and as satellites have become more digitized and software-driven, the attack surface has expanded. There are a variety of methods adversaries can use to disrupt, disable, destroy, or maliciously control satellite or their ground-based systems which command/control the satellites. The methods range from “script kiddie” attacks, individuals on the ground system, to nation-state level attacks, including supply chain intrusions or space-based attacks. A cyber-attack is not a monolithic threat, it can take many forms, have diverse entry and exploitation vectors, and can enable a host of crippling effects when triggered.

When understanding cybersecurity for space systems it is important to decompose the problem down in a basic understanding. At the most basic level, a satellite and the associated ground system can be viewed as nothing more than two computers networked together over a Radio Frequency link. Both are required for the space system to operate correctly and therefore a successful cyber-attack on either may disrupt, deny, degrade, deceive, or destroy the system. Though the specific objectives of a cyber-attack may require access to one computer or the other, access to one may be leveraged to gain access to the other computer. For example, if the goal is to destroy (or permanently disable) the satellite, an attacker may access the ground system and then leverage the RF-link to issue a command to the satellite that will result in its demise. In other words, attacking the ground can enable an attack on the satellite. Just as an attacker may target the ground network or the satellite with a cyber-attack, they also may target the satellite’s payload (i.e., sensor(s)). The threats and vulnerabilities for each aspect of the space system differs thereby requiring different security implementations to secure each.

A cyber-attack is particularly attractive for adversaries to develop and leverage in time of conflict. For a satellite, the boundary is often thought to be the communications link, i.e., the radio frequency link, or the ground system in general. If the boundary is breached, little internal protection currently exists within the satellite and an adversary can operate unhindered inside the system, in a similar way to the early days of traditional cybersecurity when border firewalls were the only protection from intrusion. Well-protected terrestrial IT systems are now designed with defense-in-depth principles.

Both large traditional developments and more modern rapidly developed space systems should ensure that they have a cyber-hardened design with defense-in-depth throughout. In the traditional sense, when cybersecurity protections have been deployed, the focus has commonly been on the ground segment with little research or guidance on securing the space segment, i.e., the satellite. A space system should have cybersecurity protections applied across the space architecture, which will aid in reducing the likelihood of a successful cyber-attack on a satellite.

Historically, satellites have been considered relatively safe from cyber threats but with space cyber threats emerging from nation-state actors, government and industry stakeholders identified that additional defenses should be implemented. Space-centric cybersecurity standards and governance have been slow to materialize and are lagging behind the growth of the cyber threat.

Defense-in-depth techniques for space system protection must be adopted across the government, industry, and international community to ensure space systems are resilient to cyber compromise. Potential solutions should include increased cooperation across these domains and require a blend of policy, standards, and technical solutions.

We are entering into an era of space-based capabilities that are not driven by government therefore do not fall under existing legislation nor governance. Currently, there are gaps on multiple fronts with respect to policy and technical standards. On the government civilian side, the majority of space systems were developed under existing cybersecurity legislation like the Federal Information Security Modernization Act (FISMA) or Federal Information Processing Standards Publication (FIPS) that are generally applied for information technology systems. However, commercial space has no binding legislation or oversight when it comes to the development and operations of space-based capabilities. We are entering into an era of space-based capabilities that are not driven by government therefore do not fall under existing legislation nor governance. The closet policy in existence that covers commercial space is SPD-5, but that policy is non-binding therefore is treating mostly as informational. This lack of policy and governance is also reflected at the standards and best practices level. Currently there are no industry recognized standards for cybersecurity in space system development and operations, especially for the satellite itself. Various standards and best practices exist for elements within the space architecture but there is currently a gap within the community that needs filled for commercial space.

One recent effort to fill the standards and best practices gap was through the government agency sponsored, publicly releasable Technical Operation Report by the Aerospace Corporation. This report documented a threat-informed risk mitigation strategy to protect satellites. The report titled *Cybersecurity Protections for Spacecraft: A Threat Based Approach* provides government and industry a background of space system cybersecurity and the state of existing standards, the concepts of defense-in-depth protection necessary to protect satellites, and then a threat-oriented approach to space cyber risk assessment. The ultimate result of this analysis is a set of products that define risk driven requirements to utilize during acquisition and operations for better space system protection.

In a similar vein NIST has released two documents (**NISTIR 8401** and **NISTIR 8270**) depicting how to leverage NIST's Cybersecurity Framework (CSF) for commercial space systems but these documents are currently circulating for comments and not officially released. It should be noted that these are not standards and are meant to introduce the topic of cybersecurity. For example, NISTIR 8270 states "this report provides a general introduction to cybersecurity risk management for the commercial satellite industry as they seek to start managing cybersecurity risks in space." NISTIR 8401 begins to decompose the cybersecurity problem more, but it only addresses how to apply the Cybersecurity Framework to the creation of a profile for the ground segment with "an emphasis on the command and control of satellite buses and payloads." While both of these documents are good places to start the conversation, there continues to be a gap in industry wide adopted and community standards and best practices for cybersecurity across all three segments of the space system. Not only are technical standards lacking, but there are also significant gaps in technical cybersecure solutions across the space architecture. The solutions that do exist do not allow for the integration of systems across multiple vendors/contractors

which drives up costs and can increase vulnerabilities due to the poor integration. Many of the security solutions developed for space technology are proprietary one-off developments and lack ability to integrate. For most commercial space systems, they need to vertically integrate, which is not scalable. Lack of cybersecurity research and development is what is preventing horizontal integration of space technology. Advancements of cybersecurity with space technology is siloed and fragmented and more collaboration is needed which is why entities like the Space ISAC are important moving forward.

More concerted efforts are needed to investigate and address the growing threat of cyber-attacks against space systems. The increasing digitization and use of autonomy has broadened the cyber-attack surface on space systems. As Aerospace focuses its strategic research towards space technology protection, more research is needed on how to secure advanced capabilities in space systems. These capabilities include autonomous and artificial intelligence, fully networked constellations, and deeper space capabilities beyond traditional orbital regimes. There is a need to mature research on applicable threats to space systems and appropriate protections of space technology in the United States critical infrastructure.

As these standards and best practices are documented and shared, collaboration on the international stage is also needed. International governance and a means for engagement with global commercial partners and agencies is needed as well. For example, there are major supply chain dependencies globally and we have few ways to convey United States cybersecurity best practices to foreign audiences who may be critical to these supply chains. Publicizing best practices for international adoption and establishing an information exchange conduit can help reduce the risk of supply chain intrusions which contends to be a substantial threat to space systems in the coming years.

In summary the following short-list of items describes the current gaps in relation to cybersecurity of space technology.

- Critical need to protect space technology and the need to create a dedicated space technology sector as one of the nation's critical infrastructure sectors
- The disjointed oversight and governance of cybersecurity for space technology
- The only space cyber policy is SPD-5. This is non-binding and treated mostly as informational
    - Even with SPD-5 there still are significant gaps in technical cybersecure solutions, standards, and best practices. Lack of cybersecurity information sharing, and research and development are what is preventing advancement of technical cybersecurity solutions for space systems. Many of the efforts within space-cyber are siloed and fragmented.
- The United States needs to work towards a global consensus through stronger collaboration among space system manufacturers, suppliers, owners and operators.
- Rapid information sharing to the entire space technology sector about threats, vulnerabilities and corrective actions is a must
    - This is a primary focus for the Space Information Sharing and Analysis Center but better collaboration across government and internationally is needed

- There are little to no security focused capabilities for on-board the satellite (i.e., monitoring, logging, and alerting). More advancement is needed on understanding the threats and building the mitigating security on the satellite vice depending on the ground to limit access to the satellite.
    - There are also gaps on the ground as well due to the fact capabilities are immature for monitoring ground system compromise for malicious commanding to the satellite.
- There is a lack of technical focus on validating security implementations in space system. Emerging security validation revolves around compliance or paperwork driven review. A lack of technical evaluation creates opportunities for vulnerabilities to be missed in the actual system implementations that will be attacked.
- Supply chain risk management on availability and integrity continues to be a challenge, especially with global supply chains of specialized equipment.
- Insider threats are also rarely considered and often considered to be mitigated by personnel security/background checks, but it takes cyber controls in addition to the personnel ones to effectively reduce insider risk.

Thank you again for this opportunity to testify on this important topic and I look forward to your questions.