EXPLORING CYBER SPACE: CYBERSECURITY ISSUES FOR CIVIL AND COMMERCIAL SPACE SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON SPACE AND AERONAUTICS

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

OF THE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JULY 28, 2022

Serial No. 117–66

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
48–138PDF WASHINGTON : 2023

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
SUZANNE BONAMICI, Oregon
AMI BERA, California
HALEY STEVENS, Michigan,
Vice Chair
MIKIE SHERRILL, New Jersey
JAMAAL BOWMAN, New York
MELANIE A. STANSBURY, New Mexico
BRAD SHERMAN, California
ED PERLMUTTER, Colorado
JERRY McNERNEY, California
PAUL TONKO, New York
BILL FOSTER, Illinois
DONALD NORCROSS, New Jersey
DON BEYER, Virginia
CHARLIE CRIST, Florida
SEAN CASTEN, Illinois
CONOR LAMB, Pennsylvania
DEBORAH ROSS, North Carolina
GWEN MOORE, Wisconsin
DAN KILDEE, Michigan
SUSAN WILD, Pennsylvania
LIZZIE FLETCHER, Texas

FRANK LUCAS, Oklahoma,
Ranking Member
MO BROOKS, Alabama
BILL POSEY, Florida
RANDY WEBER, Texas
BRIAN BABIN, Texas
ANTHONY GONZALEZ, Ohio
MICHAEL WALTZ, Florida
JAMES R. BAIRD, Indiana
DANIEL WEBSTER, Florida
MIKE GARCIA, California
STEPHANIE I. BICE, Oklahoma
YOUNG KIM, California
RANDY FEENSTRA, Iowa
JAKE LaTURNER, Kansas
CARLOS A. GIMENEZ, Florida
JAY OBERNOLTE, California
PETER MEIJER, Michigan
JAKE ELLZEY, TEXAS
MIKE CAREY, OHIO

Subcommittee on Space and Aeronautics

HON. DON BEYER, Virginia, *Chairman*

ZOE LOFGREN, California
AMI BERA, California
BRAD SHERMAN, California
ED PERLMUTTER, Colorado
CHARLIE CRIST, Florida
DONALD NORCROSS, New Jersey

BRIAN BABIN, Texas,
Ranking Member
MO BROOKS, Alabama
BILL POSEY, Florida
DANIEL WEBSTER, Florida
YOUNG KIM, California

CONTENTS

July 28, 2022

Opening Statements

Witnesses:

Appendix: Answers to Post-Hearing Questions

EXPLORING CYBER SPACE: CYBERSECURITY ISSUES FOR CIVIL AND COMMERCIAL SPACE SYSTEMS

THURSDAY, JULY 28, 2022

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON SPACE AND AERONAUTICS,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:04 a.m., in room 2318 of the Rayburn House Office Building, Hon. Don Beyer [Chairman of the Subcommittee] presiding.

SUBCOMMITTEE ON SPACE AND AERONAUTICS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

HEARING CHARTER

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

July 28th, 2022
10:00 a.m. Eastern Time
Hybrid: 2318 Rayburn House Office Building and Online via Zoom

PURPOSE

The purpose of the hearing is to examine cybersecurity for civil and commercial space systems, including current and potential cybersecurity risks, the status of policies and guidance regarding cybersecurity for space systems, and opportunities for facilitating and strengthening cybersecurity for civil and commercial space systems, among other issues.

WITNESSES

- **Dr. Theresa Suloway**, Space Cybersecurity Engineer, The MITRE Corporation
- **Mr. Matthew Scholl**, Chief, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Brandon Bailey**, Senior Project Leader, Cyber Assessments and Research Department, The Aerospace Corporation

OVERARCHING QUESTIONS

- What are the range of issues regarding commercial and civilian space systems and cybersecurity that need to be addressed?
- What is needed to support the strengthening of cybersecurity for civil and commercial space systems?
- What is the status of the workforce and pipeline for space cybersecurity, and to what extent does the workforce need expertise in both space systems and cybersecurity?
- What is the role of standards for cybersecurity for commercial space systems and what is the status of standard development for such systems?
- To what extent do government entities coordinate and collaborate on cybersecurity issues in space systems?
- What can be done to encourage commercial companies to adopt cybersecurity principles into their space systems?

BACKGROUND

The space industry touches many aspects of citizens' everyday lives and supports the global economy. Space assets provide positioning, navigation, and timing services that enable navigation applications and telecommunication services. Remote sensing assets support improvements in agriculture through moisture monitoring and in the oil and gas industry through more accurate monitoring of methane leaks.[1] Global navigation satellite systems, such as the Global Positioning System, enable financial services such as ATM transactions.[2] Disruption of these and other space services and activities could have significant economic and societal impacts.

In addition, as Federal government agencies engage in partnerships with commercial entities and use commercial space services, ensuring that such systems are secure from cyber threats is an important factor in the implementation of government missions. For example, the National Aeronautics and Space Administration (NASA) uses commercial providers to provide cargo and crew transportation services to the International Space Station. NASA plans to retire its constellation of Tracking and Data Relay Satellites, which provide communications capabilities to NASA and other government agencies, and procure communications services from the commercial sector.[3] In addition, the National Oceanic and Atmospheric Administration (NOAA) procures commercial Earth remote sensing data to supplement NOAA satellite weather data in support of its operational weather forecasting mission.

Cyber threats for commercial space systems could also have significant effects on the global space economy. From 2005 to 2020, the global space economy grew from $161 billion to $447 billion. The majority of growth has been and is projected to be in the commercial space sector. [4]

Cybersecurity for Space Systems

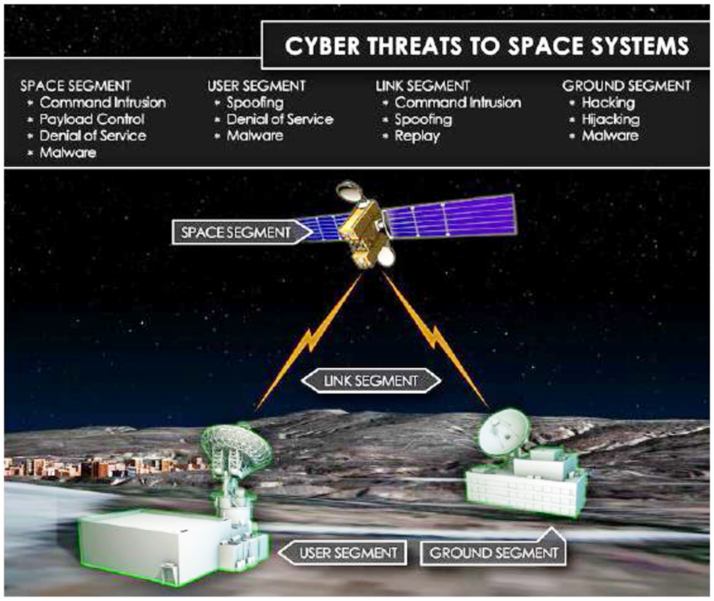
Space systems are composed of multiple segments: ground stations that operate the satellite in space; the communications and command link between the ground station and the satellite; the space segment including the satellite, its payload and spacecraft; and the user segment, which is also linked to the space segment and uses the data it provides. Each segment of a space system is exposed to different cybersecurity risks, as shown in the figure below, and mitigations differ across the type of segment, the lifecycle of the system, and the operator's risk posture.

[1] The Invisible Transformation of Global Industries – Part 1, Space Capital, Available at: https://www.spacecapital.com/publications/invisible-trans-global-industries-part-1

[2] The Invisible Transformation of Global Industries – Part 2, Space Capital, Available at: https://www.spacecapital.com/publications/invisible-trans-global-industries-part-2

[3] https://www1.grc.nasa.gov/space/communications-services-program/

[4] The Space Report 2022 Quarter 1, Space Foundation



Source: Defending Spacecraft in the Cyber Domain (The Aerospace Corporation. Nov. 2019)

Within the federal government, the National Institute of Standards and Technology (NIST) issues cybersecurity guidance for Federal government agencies and critical infrastructure owners and operators that can, when applied, strengthen the cybersecurity of their systems. In particular, NIST, under direction from Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and the Cybersecurity Enhancement Act of 2015, has developed the Cybersecurity Framework to identify and develop risk frameworks for voluntary use by critical infrastructure owners and operators.[5,6]

CYBERSECURITY THREATS TO SPACE SYSTEMS

Cybersecurity threats against space systems are myriad and evolving. Traditionally, cybersecurity for space systems has concentrated on the ground segment, which largely resembled other information technology systems.[7] Spacecraft themselves were not considered highly susceptible to cyber-attacks because of their unique hardware and software architectures and because physical access to a spacecraft after launch was highly unlikely.[8] However, as the

[5] See *15 USC Sec. 272 (e)(1)(A)(i)*. The Cybersecurity Engagement Act of 2014 (S. 1353) became public law 113-274 on December 18, 2014 and may be found at https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[6] Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, Available at: https://www.nist.gov/cyberframework/framework.

[7] Cybersecurity Protections for Spacecraft: A Threat Based Approach, The Aerospace Corporation, April 29, 2021

[8] Cybersecurity Protections for Spacecraft: A Threat Based Approach, The Aerospace Corporation, April 29, 2021

understanding of cyber threats has evolved, the range of cyber threats has expanded to include all segments of the space system.

Cybersecurity risks to commercial space systems have recently been highlighted due to the commercial communications and remote sensing sectors' support during the war in Ukraine and subsequent attacks on their systems. For example, a cyber-attack on Viasat's modems in Ukraine and other parts of Europe resulted in temporary loss of service for tens of thousands of customers throughout Europe. [9]

Examples of potential and realized cybersecurity threats to space systems include:

- Cyber weapons developed and targeted to specific spacecraft systems.[10]
- Potential vulnerabilities in the supply chain.[11]
- Hacking of ground systems, causing service disruptions to commercial and government customers, as seen in the recent Viasat hack.[12]
- Command intrusion into an operational satellite presenting potential physical risks to other satellites and the orbital ecosystem.
- Spoofing of the link between the satellite and the user, providing false information to the user.[13]
- Disruption or intentional or unintentional manipulation of signals.

SPACE POLICY DIRECTIVE-5 (SPD-5) CYBERSECURITY PRINCIPLES FOR SPACE SYSTEMS

Issued in September 2020 SPD-5 describes government policy regarding cybersecurity in space systems.[14] It states that cybersecurity principles that apply to terrestrial systems also apply to space systems and directs the government to work with industry to establish cybersecurity norms and behaviors throughout the industrial base for space systems.

Principles related in the policy include:

- Space systems should be developed and operated using risk-based cybersecurity-informed engineering.

[9] On 24 February 2022, a multifaceted and deliberate cyber-attack against Viasat's KA-SAT network resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service. Viasat is a communications company that provide satellite broadband internet services. See more: https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[10] Cybersecurity Protections for Spacecraft: A Threat Based Approach, The Aerospace Corporation, April 29, 2021

[11] Space Information and Sharing Center Overview at CISA Advanced Threat Technical Exchange. Available at: https://s-isac.org/resources/

[12] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/-

[13] Defending Spacecraft in the Cyber Domain, The Aerospace Corporation, November 2019, Available at https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.

[14] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, September 4, 2020, Available at: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

- Space systems operators should protect against unauthorized access to space vehicle functions, communications jamming and spoofing, and should protect ground systems through practices that align with NIST's Cybersecurity Framework.
- Space systems owners and operators should develop and implement cybersecurity plans that ensure operators or automated control center systems can retain control or recover control of their space vehicles.

The policy encourages space system owners and operators to collaborate through an Information Sharing and Analysis Center (ISAC), and states that security measures should be effective while permitting space system owners and operators to manage according to their risk tolerances, as consistent with mission requirements.

CYBERSECURITY STANDARDS FOR COMMERCIAL SPACE SYSTEMS AND INFORMATION SHARING

A variety of entities have published cybersecurity standards for space systems, including the Committee on National Security Systems—an intergovernmental organization that sets policy for U.S. security systems— for national security space systems,[15,16] the Consultative Committee for Space Data Systems—a multi-national forum for the development of standards for spaceflight—for international civilian space systems,[17,18] the Aerospace Industries Association for Department of Defense space systems,[19] and NASA for their space systems.[20]

In addition, in response to direction in SPD-5, the Space Information Sharing and Analysis Center (Space ISAC) was established to encourage collaboration and coordination regarding cybersecurity threats across the global space industry.[21] The Space ISAC is a private, non-profit organization that is funded by member companies who are in turn granted access to cybersecurity trainings and resources. Similar ISACs have been created for other sectors, including aviation, communications, energy management, and financial services. The Space ISAC plans to establish a Watch Center that would allow members access to unclassified, real-time cyber threat information.

[15] Security Categorization and Control Selection for National Security Systems Instruction No. 1253, The Committee on National Security Systems, March 27, 2014, Available at: https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf.

[16] National Information Assurance Instruction for Space Systems Used to Support National Security Missions Instruction No. 1200, The Committee on National Security Systems, May 7, 2014, Available at: https://www.cnss.gov/CNSS/openDoc.cfm?wrwBe/vSzqs7t2cCcl82Hg==.

[17] CCSDS Cryptographic Algorithms CCSDS 352.0-B-2, The Consultative Committee for Space Data Systems, August 2019, Available at: https://public.ccsds.org/Pubs/352x0b2.pdf.

[18] Network Layer Security Adaptation Profile CCSDS 356.0-B-1, The Consultative Committee for Space Data Systems, June 2018, Available at: https://public.ccsds.org/Pubs/356xb1.pdf.

[19] Critical Security Controls for Effective Capability in Cyber Defense, NAS 9933, Aerospace Industries Association, Available at: http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf.

[20] Space System Protection Standard, National Aeronautics and Space Administration, October 29, 2019, Available at: https://discovery.larc.nasa.gov/PDF_FILES/2019AO/nasa-std-1006.pdf

[21] https://s-isac.org/about-us/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) GUIDANCE

In response to SPD-5, NIST has developed three documents providing voluntary guidance to commercial space companies to help them apply NIST's Cybersecurity Framework to their space systems.[22] The three documents were formulated with the input of commercial industry. The three documents are:

- *Introduction to Cybersecurity for Commercial Satellite Operations*: focuses on introducing NIST's cybersecurity framework to commercial space systems.[23] It describes methods for applying the framework to a small portion of commercial satellite operations, creates an example framework of desired security outcomes, and describes a set of cybersecurity outcomes, requirements, and suggested controls.
- *Foundational Position, Navigation, and Timing (PNT) Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services*: provides a flexible framework for users of PNT services to manage risks when forming and using PNT signals and data.[24]
- *Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control:* creates a profile for ground segment operators to use to manage risks in the context of their own cybersecurity actions, systems architecture, and risk tolerance.[25] The goal of a profile is to supplement existing cybersecurity measures that ground segment operators have put in place to ensure resilience in their systems and to increase understanding and adoption of newer cybersecurity initiatives.

REGULATORY ENVIRONMENT

Federal agencies that have regulatory authority for aspects of commercial space activities stipulate certain cybersecurity measures as part of their respective licensing requirements to private space system operators. For example, NOAA's Commercial Remote Sensing Regulatory Affairs office, which licenses commercial remote sensing satellite systems, requires that satellites with propulsion control use encrypted communication so cyber attackers cannot take physical control of the satellite, among other cybersecurity related requirements. The Federal Aviation Administration's Office of Commercial Space Transportation, which licenses commercial space launch and reentry activities, has safety requirements for computing systems, among others. In addition, the Federal Communications Commission, which issues communications licenses for commercial satellite systems, stipulates, among other security-related requirements, that ground station facilities are protected by appropriate security measures to prevent unauthorized entry or operations.

[22] Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, Available at: https://www.nist.gov/cyberframework/framework

[23] Introduction to Cybersecurity for Commercial Satellite Operations NISTIR 8270, the National Institute of Standards and Technology, February 2022, Available at: https://csrc.nist.gov/publications/detail/nistir/8270/draft.

[24] Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Service NISTIR 8323, the National Institute of Standards and Technology, February 2021, Available at: https://csrc.nist.gov/publications/detail/nistir/8323/final

[25] Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control NIST IR 8401, the National Institute for Standards and Technology, April 2022, Available at: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf

Chairman BEYER. This hearing will come to order. Without objection, the Chairman is authorized to declare a recess at any time.

And before I deliver my opening remarks, I want to note that, today, the Committee is meeting both in person and virtually. And I want to announce a couple of reminders to the Members about the conduct of this hearing. First, Members and staff who are attending in person may choose to be masked, but it is not a requirement. However, any individual with symptoms, a positive test, or exposure to someone with COVID–19 should wear a mask while present.

Members who are attending virtually should keep their video feed on as long as they are present in the hearing. Members are responsible for their own microphones. Please keep your microphones muted unless you are speaking. And finally, if Members have documents they wish to submit for the record, please email them to the Committee Clerk, whose email address was circulated prior to the hearing.

So good morning, and welcome to today's hearing "Exploring Cyberspace: Understanding Cybersecurity Issues for Civil and Commercial Space Systems." I want to welcome our witnesses, both in person and virtual. We're pleased to have you with us.

Getting to space and operating there involves risk. From the launch itself to micrometeoroids, orbital debris, and geomagnetic storms, space system developers and operators must mitigate against multiple risks that can impact their satellites. But today's hearing focuses on a much more nefarious risk: cyber threats to civil and commercial space systems. These risks have taken a center stage since the public announcement of a malicious Russian attack in February 2022 on Viasat's satellite internet user modems. The hack affected thousands of customers in Ukraine and tens of thousands across Europe. Other reports cited jamming of Starlink space broadband ground terminals, which were sent to Ukraine when its communications were disrupted by the Russian invasion.

While the recent hacks have highlighted the issue, cyber threats to space systems are not new. In 2015, the Congressionally-established U.S.-China Economic Security and Review Commission reported on hacks in 2007 and 2008 to the Landsat–7 satellite. The Commission also noted that cyber actors targeted NASA's (National Aeronautics and Space Administration's) Terra Earth observation satellite on two occasions in 2008. The actors demonstrated, quote, "the steps required to command the satellite," unquote, but did not do so.

In 2014, a cyber attack on the National Oceanic and Atmospheric Administration's, NOAA's, satellite information and weather service systems actually led the agency to stop satellite transmission of weather data to the National Weather Service for two days while it responded to the incident.

These hacks perpetrated by bad actors are chilling and serious. The importance of addressing them is amplified as our reliance on space for in-space and terrestrial infrastructure and services continues to grow.

As examples, NOAA plans to procure space situational awareness data from commercial providers, and NASA plans to procure commercial space-based communication services to meet many of its communications requirements.

To date, the government and Congress have taken steps to address the matter.

In December 2020, the government issued Space Policy Directive (SPD)–5, "Cybersecurity Principles for Space Systems." In May 2021, Chairwoman Johnson, Ranking Member Lucas, myself, and Ranking Member Babin requested that the GAO, the Government Accountability Office, conduct a review of the cybersecurity risk to the sensitive data associated with NASA's major projects and spaceflight operations. That review is now underway.

Other Members of Congress have introduced legislative proposals on space and cybersecurity.

More recently, following the Viasat incident, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI (Federal Bureau of Investigation) issued an alert on strengthening cybersecurity of satellite communication network providers and customers. The National Security Agency also issued a cybersecurity advisory to protect small ground terminals used to transmit and receive satellite communications. And the Department of Commerce's National Institute of Standards and Technology (NIST) has issued guidance on cybersecurity for commercial space systems.

Today's hearing will give us an opportunity to review these efforts and the overall landscape of cybersecurity for civil and commercial space systems, including, what is the range of threats today? What is the status of the implementation of space director—Space Policy Directive–5? What role should the Federal Government have, and is there an agency in charge of space cybersecurity? And what are the issues for Congress?

We need to make every effort to understand what further actions can be and should be taken to strengthen cybersecurity for civil and commercial space systems, including commercial space systems that provide mission-critical government data and services. Malicious disruptions to such systems would have significant impacts to critical services, our economy, and the growing $447 billion global space economy, including everything from weather and environmental forecasting, to forestry management, to communications, space science, and national security.

I look forward to hearing from our expert witnesses on this important issue. And before I close, I want to note the groundbreaking progress that will be made with the House's voting on the Senate-passed *CHIPS and Science Act of 2022*. This act includes the first NASA authorization in five years. And I think I'm very proud that this NASA authorization includes many of the changes, the recommendations from both the GAO report on NASA and the Inspector General (IG) report on NASA. The core set of provisions provide direction across NASA's portfolio that will support the agency in continuing to lead, inspire, discover, explore, and carry the ambitious and challenging space and aeronautics missions.

[The prepared statement of Chairman Beyer follows:]

Good morning, and welcome to today's hearing, *Exploring Cyber Space: Understanding Cybersecurity Issues for Civil and Commercial Space Systems.*

I want to welcome our witnesses. We are pleased to have you with us both in person and virtually.Getting to space and operating there involves risk. From the launch itself, to micrometeoroids, orbital debris, and geomagnetic storms, space system developers and operators must mitigate against multiple risks that can impair their satellites.

Today's hearing focuses on a more nefarious risk—cyber threats to civil and commercial space systems. The risks have taken center stage since the public announcement of a malicious Russian attack in February 2022 on Viasat's satellite internet user modems. The hack affected thousands of customers in Ukraine and tens of thousands across Europe. Other reports cited jamming of Starlink's space broadband ground terminals, which were sent to Ukraine when its communications were disrupted by the Russian invasion.

While the recent hacks have highlighted the issue, cyber threats to space systems are not new. In 2015, the Congressionally-established U.S.-China Economic Security and Review Commission reported on hacks in 2007 and 2008 to the Landsat–7 satellite. The Commission also noted that cyber actors targeted NASA's Terra Earth observation satellite on two occasions in 2008. The actors demonstrated the "steps required to command the satellite" but did not do so.

In 2014, a cyber-attack on the National Oceanic and Atmospheric Administration's satellite information and weather service systems led the agency to stop satellite transmission of weather data to the National Weather Service for two days while it responded to the incident.

These hacks perpetrated by bad actors are chilling and serious. The importance of addressing them is amplified as our reliance on space for in-space and terrestrial infrastructure and services continues to grow.

As examples, NOAA plans to procure space situational awareness data from commercial providers and NASA plans to procure commercial space-based communications services to meet many of its communications requirements.

To date, the government and Congress have taken steps to address the matter.

In December 2020, the government issued Space Policy Directive–5, "Cybersecurity Principles for Space Systems."

In May 2021, Chairwoman Johnson, Ranking Member Lucas, myself, and Ranking Member Babin requested that Government Accountability Office conduct a review of the cybersecurity risks to the sensitive data associated with NASA's major projects and spaceflight operations. That review is now underway.

Other Members of Congress have introduced legislative proposals on space and cybersecurity.

More recently, following the Viasat incident, the Cybersecurity and Infrastructure Security Agency and the FBI issued an alert on strengthening cybersecurity of satellite communications network providers and customers. The National Security Agency also issued a cybersecurity advisory to protect small ground terminals used to transmit and receive satellite communications. And the Department of Commerce's National Institute of Standards and Technology has issued guidance on cybersecurity for commercial space systems.

Today's hearing will give us an opportunity to review these efforts and the overall landscape of cybersecurity for civil and commercial space systems, including

- What is the range of threats today?
- What is the status of implementation of Space Policy Directive 5?
- What role should the Federal government have, and is there an agency in charge of space cybersecurity?
- And, what are the issues for Congress?

We need to make every effort to understand what further actions can be and should be taken to strengthen cybersecurity for civil and commercial space systems, including commercial space systems that provide mission-critical government data and services.

Malicious disruptions to such systems would have significant impacts to critical services, our economy, and the growing $447 billion global space economy, including everything from weather and environmental forecasting to forestry management, communications, space science, and national security.

I look forward to hearing from our expert witnesses on this important issue.

Before I close, I want to note the ground-breaking progress that will be made with the House's voting on the Senate-passed *CHIPS and Science Act of 2022.*

This Act includes the first NASA Authorization in five years. The core set of provisions provide direction across NASA's portfolio that will support the agency in continuing to lead, inspire, discover, explore, and carry out ambitious and challenging space and aeronautics missions.

Chairman BEYER. Let me now turn to my friend, the good doctor from Houston and the Ranking Member, Mr. Babin.

Mr. BABIN. Thank you, Chairman Beyer. I really appreciate that very much. Good morning. Thanks for holding this important hearing.

We've held a number of hearings on space cybersecurity over the last several years and unfortunately learned of many cybersecurity incidents related to civil and commercial space. The 2011 U.S.-China Economic Security Review Commission report to Congress indicated that hackers interfered with USGS's (United States Geological Survey's) Landsat–7 satellite in October 2007 and also in July 2008, and NASA's Terra satellite in June 2008 and October 2008. In 2014, we also heard of intrusions into NOAA's weather and satellite network. A 2019 report from the NASA IG indicated that NASA Information Technology Security Managers remain concerned about potential infiltration into NASA's spaceflight systems to acquire launch codes and flight trajectories of spacecraft. More recently, senior NASA officials stated that the hack of a SolarWinds software of—excuse me—of SolarWinds software was a big wakeup call. Just a few months ago, the Secretary of State issued a formal statement attributing a cyber attack on a commercial satellite communication network to Russia.

With the proliferation of commercial space operations and NASA's increased use of commercial services, this hearing is a timely update on the topic of cybersecurity in civil and commercial space. It is a continuation of longstanding, bipartisan oversight. Last year, the Committee and Space Subcommittee Chairs and Ranking Members jointly asked GAO to review NASA and NASA contract cybersecurity, and we look forward to reviewing that work very soon.

The executive branch is also focused on space cybersecurity issues. In September 2020, the Trump Administration issued Space Policy Directive–5, which outlined the U.S. Government's first cybersecurity policy for space systems. Earlier this year—excuse me—earlier this spring, the Department of Homeland Security (DHS) updated their space policy for the first time since 2011. Last year, the Cybersecurity and Infrastructure Security Agency, or CISA, announced the formation of the Space Systems Critical Infrastructure Working Group to bring together stakeholders from across the sector to minimize risks to space systems. Industry coalitions are emerging to provide private sector information sharing and collaboration without government intervention.

And last but not least, NIST continues to provide world-class services and standards, as they have done since the 1970's on cybersecurity. All of these activities promote a bottoms-up approach to private sector cybersecurity issues that are focused on information sharing rather than proscriptive regulations. This is the correct path, as it ensures the industry remains at the cutting edge of innovation rather than generations behind our adversaries like China.

As we continue our bipartisan oversight of this important topic, we should also reach out to space operators, launch providers, prime contractors, component subcontractors, software providers, antenna and ground station operators, and even end users to ensure that we understand the breadth of this topic. This will help inform how Congress responds to future questions such as whether space should be listed as an additional critical infrastructure protection sector. This is a complex question. Many aspects of space are already covered by other sectors like communications, defense industrial base, critical manufacturing, information technology, government facilities, emergency services, financial services, and even food and agriculture. Some space activities like suborbital tourism may not rise to the definition of critical. For this reason, both the Trump and Biden Administrations have chosen not to add space as an additional sector, instead focusing instead on critical functions.

I look forward to hearing from our witnesses and continuing our conversation on how we as a nation can best secure our space cyber domain while also maintaining our leadership in space commerce. So thank you, Mr. Chairman, and I yield back the balance of my time.

[The prepared statement of Mr. Babin follows:]

Good morning and thank you Mr. Chairman for holding this important hearing.

We've held a number of hearings on space cybersecurity over the last several years, and, unfortunately, learned of many cybersecurity incidents related to civil and commercial space. The 2011 US-China Economic Security Review Commission report to Congress indicated that hackers interfered with USGS's Landsat 7 satellite in October 2007 and July 2008 and NASA's Terra satellite in June 2008 and October 2008. In 2014 we also learned of intrusions into NOAA's weather and satellite network. A 2019 report from the NASA IG indicated that NASA information technology security managers remain concerned about potential infiltration into NASA's space flight systems to acquire launch codes and flight trajectories of spacecraft. More recently, senior NASA officials stated that the hack of SolarWinds software "was a big wakeup call." Just a few months ago, the Secretary of State issued a formal statement attributing a cyber-attack on a commercial satellite communication network to Russia.

With the proliferation of commercial space operations and NASA's increased use of commercial services, this hearing is a timely update on the topic of cybersecurity in civil and commercial space. It is a continuation of long-standing bipartisan oversight. Last year the committee and space subcommittee chairs and ranking members jointly asked GAO to review NASA and NASA contractor cybersecurity, and we look forward to reviewing their work soon.

The executive branch is also focused on space cybersecurity issues. In September 2020, the Trump Administration issued Space Policy Directive–5 (SPD–5), which outlined the U.S. Government's first cybersecurity policy for space systems. Earlier this spring, the Department of Homeland Security updated their space policy for the first time since 2011. Last year, the Cybersecurity and Infrastructure Security Agency (CISA) announced the formation of a Space Systems Critical Infrastructure Working Group to bring together stakeholders from across the sector to minimize risks to space systems. Industry coalitions are emerging to provide private sector information sharing and collaboration without government intervention. And last, but not least, NIST continues to provide world-class services and standards—as they have done since the 1970s on cybersecurity. All these activities promote a "bottoms-up" approach to private sector cybersecurity issues focused on information sharing rather than proscriptive regulations. This is the correct path, as it ensures the industry remains at the cutting-edge of innovation rather than generations behind our adversaries.

As we continue our bipartisan oversight of this important topic, we should also reach out to space operators, launch providers, prime contractors, component subcontractors, software providers, antenna, and ground station operators, and even end-users to ensure we understand the breadth of the topic. This will help inform how Congress responds to future questions, such as whether space should be listed as an additional Critical Infrastructure Protection sector. This is a complex question. Many aspects of space are already covered by other sectors like communications, defense industrial base, critical manufacturing, information technology, government facilities, emergency services, financial services and even food and agriculture. Some space activities, like suborbital tourism may not rise to the definition of "critical." For this reason, both the Trump and Biden Administrations have chosen not to add space as an additional sector, instead focusing instead on critical "functions."

I look forward to hearing from our witnesses and continuing our conversation on how we as a nation can best secure our space cyber domain while also maintaining our leadership in space commerce. Thank you and I yield back the balance of my time.

Chairman BEYER. Dr. Babin, thank you very much.

If there are other Members who wish to submit additional opening statements, your statements will be added to the record at this point.

[The prepared statement of Chairwoman Johnson follows:]

Good morning,

Thank you, Chairman Beyer, for holding today's hearing on cybersecurity for civil and commercial space systems. And welcome to our witnesses who will be testifying today on this important topic.

Unfettered access and freedom to operate in space are vital to the advancement of the security, economic prosperity, and scientific knowledge of the United States, as emphasized in the United States National Cyber strategy. The growing threats to space assets and their supporting infrastructure is a matter of great concern for this Committee and Subcommittee.

Commercial space systems play a crucial role in the United States and world economy, and one that is expected to grow as the government realizes plans to increasingly leverage commercial space capabilities.

As was seen during the war in Ukraine with the hacking of Viasat's ground stations and subsequent communications outages, commercial space systems are exposed to cybersecurity threats that can degrade critical functions.

In addition to cyber hacks to ground systems, cyber threats to satellites and their spacecraft, users, and the links between the two could cripple many of the services necessary to modern life in the United States. Those services include remote sensing and position, navigation, and timing systems that support many sectors of our economy and national security.

We need to ensure that we understand this threat and what options we have to mitigate and address it.

As Chairman Beyer noted, the government has begun taking steps to address cybersecurity in space systems with Space Policy Directive–5, which directs the government to work with the commercial space industry to establish cybersecurity norms and behaviors. In addition, the National Institute of Standards and Technology is applying its cybersecurity framework to different segments of commercial space systems.

However, more needs to be done in this area. There are no universally accepted standards for cybersecurity in space systems. More work is also needed to translate high-level policy and guidance into practical engineering standards that commercial companies can apply to their systems.

The issues and risks surrounding this topic are numerous. I look forward to hearing from our expert panelists on what is needed to increase cyber resilience in commercial and civil space systems. Preventing the crises that would result if cyber risks were to be realized must be a priority.

Thank you, and I yield back.

Chairman BEYER. At this time, I'd like to introduce our witnesses. Dr. Theresa Suloway is a space cyber subject matter expert at the MITRE Corporation. Dr. Suloway previously served as the Department Manager at the National Cybersecurity Federally Funded Research and Development Center (FFRDC) at MITRE, sponsored by the National Institutes of Standards and Technology, or NIST. She worked with NIST on developing several NIST Interagency Reports on commercial space and also serves as an alternate board member to the Space Information Sharing Working Group. Dr. Suloway has 15 years of technical experience in the DOD (Department of Defense) and the U.S. intelligence community, guiding R&D (research and development) and operational effort—activities. So, Dr. Suloway, welcome.

Dr. Matthew Scholl, who's with us virtually, is the Chief of the Computer Security Division in the Information Technology Laboratory at the U.S. Department of Commerce's NIST. Mr. Scholl oversees a research program that cultivates trust in information technology and metrics by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry. He also co-leads NIST's participation with the Cybersecurity National and International Standards Development Organization. He is a U.S. Army veteran and currently has more than 20 years of Federal service. Welcome, Mr. Scholl.

Finally, Mr. Brandon Bailey is a Senior Cybersecurity Project Manager within the Cybersecurity Subdivision at The Aerospace Corporation. Mr. Bailey has spent much of his professional career supporting space agencies such as NASA, where he led various cybersecurity efforts. More recently, Mr. Bailey has published several articles and reports focusing on adding cybersecurity in the space systems to meet the evolving threat landscape, including a set of products that define risk-driven requirements. So, Mr. Bailey, welcome.

And as our witnesses should know, you will each have five minutes for your spoken testimony. Your written testimony, which can be much longer, will be included in the record for the hearing. When you've all completed your spoken questions—your spoken testimony, we will begin with the difficult questions. Each Member will have five minutes to question the panel.

We will start with Dr. Theresa Suloway. Dr. Suloway, the floor is yours.

TESTIMONY OF DR. THERESA SULOWAY, SPACE CYBERSECURITY ENGINEER, THE MITRE CORPORATION

Dr. SULOWAY. Thank you. Good morning, Chairman Beyer, Ranking Member Babin, and distinguished Members of the Subcommittee on Space and Aeronautics. Thank you for inviting me to testify before you on commercial space cybersecurity. Successful adoption of cybersecurity in the commercial space industry is a critically important issue, and I appreciate the opportunity to share insights from my work on this topic.

My name is Theresa Suloway. I am a Space and Cybersecurity Engineer and Project Lead with MITRE. My testimony today comes from my 15 years of technical experience working at MITRE and in the industry-guiding research and development and operational activities across government. I also serve as an active member of the Space Information Sharing and Analysis Center or ISAC.

My role with MITRE has involved support to NIST's National Cybersecurity Federally Funded Research and Development Center. This FFRDC administers NIST's National Cybersecurity Center of Excellence, or NCCOE, which MITRE has operated since 2014. I would like to make a brief statement and to submit my full remarks for the record.

When discussing space systems, it is useful to divide the landscape 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, such as global navigation systems—for example, GPS (Global Positioning System) —and internet services. The ground segment is defined by the infrastructure that supports the tasking and operation of the satellites and its payloads, including the computer networks, antennas, and industrial control systems that support transmission to the satellite. The space segment represents the satellite that is in orbit. NIST has published interagency reports to address each segment, which I co-authored in my role with MITRE.

The NIST cybersecurity framework consists of five core functions: identify, protect, detect, respond, and recover, all applicable to the space domain. First, we must identify the risks and vulnerabilities to the space ecosystem. For example, one of the most urgent cybersecurity risks that must be addressed from—for commercial space is the possibility that one or more satellites could be hijacked to cause a collision. A collision between satellites would not only destroy the satellites involved, but the resulting debris will permanently remove that orbit or region from use by any other satellite. This risk requires preemptive rather than reactive action.

As dependence on commercial space services grow, our critical infrastructure is exposed to further cascading risks from our Nation's food supply to hospital communications to energy delivery. Rural locations, which are solely dependent on commercial satellite connectivity, are at higher risks if these services are disrupted.

The ground segment is vulnerable because it is the easiest to access through traditional means. While harder to access, the space segment is vulnerable to corrupted commands or software being sent from either a trusted or malicious source. Adding encryption to the ground space link would mitigate some of the vulnerabilities by making it harder for malicious sources to send commands to the satellites.

An attacker can be successful, regardless of the measures you put in place, making monitoring key. Monitoring and cyber situational awareness need to be built in now as part of the fabric of commercial space. You can't respond to and recover from an attack you're unaware of.

The commercial space industry operates within the constraints of size, weight, power, and cost and needs to serve both customers and investors. Introducing burdensome, costly—potentially costly cyber requirements into this already high-risk, high-cost environment without a full understanding of the impacts of those requirements could force companies to move their operations abroad, affecting our Nation's standing as a leader in this burgeoning domain.

Based on my experiences and observations, I recommend the Committee consider the following actions: Incentivize adoption of best practices by investing in R&D for cybersecurity technologies for space systems. If only one requirement is applied, ensure that it is encryption and encryption modules that can upgrade to postquantum algorithms. Formalize and strengthen the government's relationship with the space ISAC. In addition, incentivize commercial space companies to share information with the space ISAC. The space ISAC's watch center, coming online in Q–4 of this year, could provide both government and industry with needed awareness. Consideration should be given to the designation of space systems as critical infrastructure, which would provide additional emphasis to the cybersecurity and resilience of civil and commercial space systems.

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

[The prepared statement of Dr. Suloway follows:]

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.

Dr. Theresa Suloway is a Space Cyber Subject Matter Expert at the MITRE Corporation. Theresa served previously as the Department Manager of the National Cyber Security Federally Funded Research and Development Center (MITRE), sponsored by the National Institute of Science and Technology. Theresa has published several papers in the area of cybersecurity for Commercial Space Systems. Most notably Theresa has worked with NIST on developing several NIST Interagency Reports (NISTIR) on Commercial Space. For the space segment, NISTIR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)); for the ground segment, NISTIR 8401 (Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control) and for the user segment, NISTIR 8323, Foundational PNT Profile | CSRC. Theresa serves as an alternate board member to the Space Information Sharing Working Group. Dr. Suloway has 15 years of technical experience in the DoD and the US Intelligence Community, guiding R&D and operational activities. Theresa holds a bachelor's degree in Aerospace Engineering from the University of Illinois at Champaign Urbana and a Master and Ph.D. in Aeronautics and Applied physics from the California Institute of Technology.

Chairman BEYER. Dr. Suloway, thank you very much.

Let me now introduce Mr. Matthew Scholl from NIST.

TESTIMONY OF MR. MATTHEW SCHOLL, CHIEF, COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. SCHOLL. Chairman Beyer, Ranking Member Babin, and Members of the Subcommittee, I am Matthew Scholl, Chief of the Computer Security Division at NIST. Thank you for the opportunity to testify today.

NIST is the home to five Nobel Prize winners with programs focused on our Nation's priorities such as AI (artificial intelligence), advanced manufacturing, the digital economy, precision metrology, quantum sciences, biosciences, and of course, cybersecurity.

In the area of cybersecurity, NIST has worked with our partners since 1972 when we published the data encryption standard. NIST's role is to provide standards, guidance, tools, data references, and testing methods that protect our Nation's information and information systems.

As stated in the 2021 U.S. Space Priorities Framework, access to and use of space is of a vital national interest. However, cyber-related threats to space assets pose increasing risk to the commercial space emerging market. Space is a high-risk environment, so cybersecurity risks involving commercial space needs to be understood and managed to ensure safe and successful operations. Physical risks to space are generally quantifiable and have the most likely potential to adversely impact businesses that operate commercial satellites. While physical risks are generally the primary risk, continued growth in commercial space operation allows us the opportunity to address cybersecurity risks as well.

As mentioned earlier, Space Policy Directive–5, the "Cybersecurity Principles for Space Systems," has established some key principles for cybersecurity in space. And it states that space systems are reliant on information systems and networks from design through launch and flight operations. These systems can be vulnerable to malicious activity. That includes spoofing of sensor data, corrupting sensor systems, jamming and sending unauthorized commands for guidance and control, the injection of malicious code, and conducting denial-of-service attacks.

In order to assist with the need to address these issues, NIST has taken some actions. Now, NIST is not a space agency, but rather a measurement and metrology agency with a long history in cybersecurity. We provide our expertise to mission owners like space operators, where we couple our cybersecurity experience and expertise with their understanding and context of the mission area in order to create our applicable and effective resources. These resources include a foundational PNT (position, navigation, and timing) profile, applying cybersecurity framework for the responsible use of position, navigation, and timing services. Executive Order (EO) 13905, strengthening our Nation's resilience through responsible use of position, navigation, and timing services, directed NIST to develop this cybersecurity profile to assist with managing risks to systems that are dependent on PNT services.

We also created the “Introduction to Cybersecurity for Commercial Satellite Operations.” This guidance provides a general introduction to cybersecurity risk management for commercial satellite operators. While it’s not intended to be comprehensive, it presents basic concepts and provides sample references for additional information on cybersecurity risk management for use by this industry.

We also created the “Satellite Ground Segment” applying the cybersecurity framework to assure satellite command and control. This guidance addresses risks specifically to the ground segment of space operations. It defines the ground segment and its components and presents mappings to relevant cybersecurity informative references to assist in the management of risk to this part of space operations.

NIST also works with our partners and has co-hosted a series of external events, for example, the Space Cybersecurity Symposium Series. NIST, working with the Department of Commerce’s Office of Space Commerce and the Department of Homeland Security, work together on a series of jointly hosted symposiums where we learn and share information about the latest cyber threats to space infrastructure. We learn from the industry’s cybersecurity experiences, we hear about their needs and their acceptable mitigation strategies.

Commercial space operations and opportunities continue to grow and provide an engine for our economy and expand our understanding of the world and the universe. This emerging nature of commercial space technologies gives us this new opportunity.

Thank you for the opportunity to discuss NIST’s activities today, and I’m pleased to answer any questions you might have.

[The prepared statement of Mr. Scholl follows:]

Testimony of

Matthew A Scholl
Chief
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space and Technology,
Subcommittee on Space and Aeronautics

on

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

July 28, 2022

Chairman Beyer, Ranking Member Babin, and Members of the Subcommittee, I am Matthew Scholl, the Chief of the Computer Security Division, of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology – known as NIST. Thank you for the opportunity to testify today on behalf of NIST on efforts to improve the cybersecurity of space operations.

NIST is home to five Nobel Prize winners, with programs focused on national priorities such as artificial intelligence, advanced manufacturing, the digital economy, precision metrology, quantum science, biosciences and, of course, cybersecurity. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST's Role in Cybersecurity

In the area of cybersecurity, NIST has worked with federal agencies, industry, international partners and academia since 1972, when it helped develop and published the Data Encryption Standard, which enabled efficiencies with security, like the electronic banking that we all enjoy today. NIST's role is to provide standards, guidance, tools, data references, and testing methods to protect information systems against threats to the confidentiality, integrity, and availability of information and services. This role was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, tribal, and territorial governments, because NIST's standards and guidelines are effective, state-of-the-art, and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

Cybersecurity and Space Challenges

As stated in the 2021 U.S. Space Priorities Framework, "[a]ccess to and use of space is a vital national interest." However, cyber-related threats to space assets (e.g., commercial satellites) and supporting infrastructure pose increasing risk to this economic promise and commercial space emerging markets.

Space is a high-risk environment in which to operate, so cybersecurity risks involving commercial space needs to be understood and managed alongside other types of risks to ensure

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

safe and successful operations. Physical risks to these operations are generally quantifiable and have the most likely potential to adversely impact the businesses that operate commercial satellites, usually occurring in low earth orbit. While these physical risks are the primary risk considerations to satellite operations, continued growth in this new commercial infrastructure allows for opportunities to address the cybersecurity risks along with the many other risk elements considered.

Memorandum on Space Policy Directive 5 (SPD-5) – Cybersecurity Principles for Space Systems, issued September 2020, establishes key cybersecurity principles to guide and serve as the foundation for America's approach to the cybersecurity of space systems. It directs U.S. Government agencies to work with commercial companies to promote these throughout the sector. SPD-5 further underscores the risks of such systems:

> "Space systems are reliant on information systems and networks from design conceptualization through launch and flight operations. Further, the transmission of command and control and mission information between space vehicles and ground networks relies on the use of radio-frequency-dependent wireless communication channels. These systems, networks, and channels can be vulnerable to malicious activities that can deny, degrade, or disrupt space operations, or even destroy satellites.
>
> Examples of malicious cyber activities harmful to space operations include spoofing sensor data; corrupting sensor systems; jamming or sending unauthorized commands for guidance and control; injecting malicious code; and conducting denial-of-service attacks. Consequences of such activities could include loss of mission data; decreased lifespan or capability of space systems or constellations; or the loss of positive control of space vehicles, potentially resulting in collisions that can impair systems or generate harmful orbital debris."[2]

NIST's Work in Space Cybersecurity

Consistent with SPD-5 and to assist with the need to address many of these issues, NIST has taken actions that help to further this opportunity to include cybersecurity risk management as part of space operations.

NIST is not a space mission agency, but a measurement and metrology agency with a long history in cybersecurity. Per our mission, we provide our expertise to mission owners, like space operators, where we couple our deep cybersecurity experience with their understanding and contextual knowledge of the mission area to create applicable cybersecurity tools, references and guidance. These resources includes:

- **Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services.** The national and economic security of the United States (US) depends on the reliable functioning of PNT services. In a 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

[2] Space Policy Directive-5; Cybersecurity Principles for Space Systems. Sept 4, 2020.

Secretary of Commerce, in coordination with the heads of Sector Risk Management 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 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.** This guidance, the *Introduction to Cybersecurity for Commercial Satellite Operations (NIST IR 8270)*, provides a general introduction to cybersecurity risk management for commercial satellite operations. While it is not intended to be comprehensive, this guidance 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. The guidance was written in response to the 2018 Cybersecurity National Strategy and in support of SPD -5.

- **Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control.** *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 SPD-5.

- **Hybrid Satellite Networks: Cybersecurity Draft Annotated Outline.** NIST recently released a draft outline applying the NIST Cybersecurity Framework to hybrid satellite networks. The publication is currently out for stakeholder review and comment.

Events: NIST has also co-hosted a number of events:

- **Space Cybersecurity Symposium Series.** NIST worked with the Department of Commerce (DOC) Office of Space Commerce and the Department of Homeland Security (DHS) on a series of jointly hosted symposiums to learn about the latest cyber threats to space infrastructure, existing space cybersecurity policies, and industry cybersecurity experience and mitigation strategies.

Conclusion

Commercial space operations and opportunities continue to grow and provide an engine for our economy and expand our understanding of the world and the universe. Space operations are, by their very nature, fraught with risks that are not present with traditional Information Technology or Operational Technology Systems. The emerging nature of commercial space technologies gives us an opportunity to address cybersecurity risks early and in a broad, integrated way. The timely availability of cybersecurity guidance, efforts alongside industry in standards bodies, sharing of cybersecurity threat information and creation of resilient and recoverable space technologies is a critical part of our support for space missions that contribute to our economy, our security, and our understanding of the universe.

NIST is proud of its role in establishing and improving cybersecurity solutions, standards, guidelines, and other resources, and of the longstanding and robust collaborations we've established with our federal government partners, private sector collaborators, and international colleagues.

Thank you for the opportunity to discuss NIST's activities related to space operations and cybersecurity. I will be pleased to answer any questions you may have.

Matthew A Scholl

Matthew Scholl is the Chief of the Computer Security Division (CSD) in the Information Technology Laboratory (ITL) at the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST). CSD, one of seven Divisions within ITL, has an annual budget of $32 million, nearly 100 federal employees, and an additional approximately 50 guest researchers from industry, universities, and foreign laboratories.

Mr. Scholl oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry.

He also co-leads NIST's participation with Cybersecurity National and International Standards Development Organizations (SDOs) and associated conformance testing programs.

Mr. Scholl has a Master's in Information Systems from the University of Maryland and a bachelor's degree from the University of Richmond.

He is a U.S. Army veteran and currently has more than 20 years of federal service.

Chairman BEYER. Mr. Scholl, thank you very much.

We'll now hear from Mr. Brandon Bailey, a NASA veteran and now with The Aerospace Corporation. Mr. Bailey?

TESTIMONY OF MR. BRANDON BAILEY, SENIOR PROJECT LEADER, CYBER ASSESSMENTS AND RESEARCH DEPARTMENT, THE AEROSPACE CORPORATION

Mr. BAILEY. Thank you. Chairman Beyer, Ranking Member Babin, and distinguished Members of the Subcommittee, thank you for inviting me to join the discussion. Within the last decade, Aerospace Corporation has been performing analysis and research on space systems cybersecurity to protect against an evolving threat landscape. I've personally spent the majority of my 16-year career focusing on cybersecurity issues with commercial and civilian space systems. My submitted written testimony goes into much more detail, but I would like to cover several aspects within this testimony describing the current gaps in relation to cybersecurity of space technology.

There's a critical need to protect space technology, which can lead to creating critical infrastructure sector for space technology. There's currently disjointed oversight in governance of cybersecurity, in addition to the lack of binding space cyber policy or widely adopted technical standards for commercial space, which is lagging behind the growth of the cyber threat. There continues to be significant gaps in technical cybersecurity solutions, technical-oriented standards and best practices for space technology, as well as the lack of cybersecurity information sharing, and research and development for space technology, as many efforts within space cyber are siloed and fragmented. This lack of research and information sharing has led to a significant lack of security-focused defensive capabilities onboard the satellites. There continues to be too much existing focus on the ground segment protections to limit access to the satellite.

The release of Space Policy Directive–5 in September 2020 and the fact we're having this hearing testifies to the importance of space technology, and cybersecurity. Space Policy Directive–5 stated that space systems contribute to the operation of the Nation's critical infrastructure, and when leveraging Presidential Policy Directive 21's definition for critical infrastructure, it's unquestionable that there is space technology that qualify for this definition.

Space technology is important for industry and government activity, as well as everyday people activities. In fact, according to the Department of Homeland Security, all 55 of the national critical functions have some sort of dependency or enabled by space technology. However, simply stating thou shalt 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 must contend with harsh environmental conditions of space, accommodate strict size, weight, and power constraints for operating in space. Therefore, ensuring a proper sector risk management agency is selected, along with support from other applicable Federal departments, agencies, and space domain-aware entities who understand the nuance of cybersecurity in addition to the space environment will be crucial to the successful implementation of identifying space technology as a critical infrastructure sector. If done properly, having a space domain-knowledgeable governance structure can help establish better cybersecurity standards and sharing information across the community.

It has been openly communicated by the Defense Intelligence Agency that adversarial nations plan to target United States-based technology via cyber means. And we're entering into an era of space-based capabilities that are not driven by government, therefore, do not fall under existing regulation or governance. With this 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.

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 simply 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.

One recent effort to fill standards and best practices gap was through the government agency-sponsored publicly releasable technical operating report by The Aerospace Corporation. This report documented the 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 on space cybersecurity and the state of existing standards, the concept of technical defense-in-depth protection necessary to protect satellites, and the threat-oriented approach to space cyber risk assessment. This report has been submitted as a part of the record with this testimony.

In summary, the need to protect space technology is very apparent. Therefore, we need to foster a whole-of-government solution working with industry to establish proper guardrails, creating binding policy and a new critical infrastructure sector for space technology and levering the space cyber-aware Federal agencies and entities like the Information Sharing and Analysis Center to improve cyber across the board will be imperative. The government sector has knowledge on how to protect space-based capabilities, but we need to foster better information sharing across the board. The United States needs to work toward a global consensus through stronger collaboration among space system manufacturers, suppliers, owners, and operators. Information sharing to the entire space technology sector about threats, vulnerabilities, corrective action is a must, which can lead to improved security across all segments of the space architecture.

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

[The prepared statement of Mr. Bailey follows:]

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.

Brandon Bailey
Senior Cybersecurity Project Manager
Aerospace Corporation

Mr. Bailey currently works for the Aerospace Corporation within the Cybersecurity Subdivision as a Senior Cybersecurity Project Manager and is a former GS-15 at NASA where he led various cybersecurity efforts and was awarded NASA's Exceptional Service Medal for his landmark cybersecurity work in 2019. Mr. Bailey has spent much of his 16-year professional career supporting space agencies like National Aeronautics and Space Administration (NASA). More recently Mr. Bailey has published articles and reports focusing on adding cybersecurity into space systems to meet the evolving threat landscape. Specifically, Mr. Bailey authored a report titled *Cybersecurity Protections for Spacecraft: A Threat Based Approach* which was outlines concepts of defense-in-depth protection necessary to protect spacecraft, and then a threat-oriented approach to space cyber risk assessment. The ultimate result of this report is a set of products that define risk driven requirements to utilize during acquisition and operations for better space system protection.

Chairman BEYER. Mr. Bailey, thank you very much.

We'll now begin a round of questions. I first want to make sure that you're not discouraged that there's not a full dais up here. You know, with—Congress goes out—the House goes out tomorrow in theory for five or six weeks, so everyone's packing everything in to these last days. And especially with the huge *CHIPS and Science Act of 2022* bill, which is dramatic in so many different ways, and which in theory will be coming for a vote later today. But so—but please know that there are tens of thousands of people watching C–SPAN across the country, and many—this is on TV in many offices across the Hill right now. And hopefully, more people will come up to answer—ask questions. Otherwise, Brian and Mr. Posey and I will grill you for a long time.

Dr. Suloway, let me start with you. You mentioned three following actions. One was the incentive bias option—adoption of best practices, and you specifically said encryption modules that can upgrade to post-quantum algorithms. Do the encryption modules exist right now that—at industrial scale that can be adopted by the commercial and the government users? And since no one's broke through on the quantum algorithms yet, I don't think, how do you ensure that your encryption is going to be upgradeable when you don't know how the quantum computing is yet going to work?

Dr. SULOWAY. Thank you for the question. So as far as the the need for encryption, there are often software-only encryption systems that you can deploy on your satellite, so you wouldn't have to physically buy a piece of hardware and and put it on your satellite. You would still need to be able to support the compute functions of that encryption software.

From a perspective of post-quantum encryption, the algorithms have actually already—are being published by NIST, and so there are some of these available. I think the the concern with the post-quantum encryption and why I put that in my testimony is because we want to be able to upgrade in the future so satellites being launched cannot be physically altered once they're in space. And so the driver to try and get the capability in there, even if the technologies aren't available yet.

Chairman BEYER. Yes, we certainly—we've had a lot of hearings in this Committee on blockchain, for example, which is just fascinating until you realize that blockchain's strength and impenetrability may go away right away once quantum computing happens.

But, by the way, we're all a little intimidated by a Ph.D. in aeronautics and applied physics at Caltech, you know. Almost nothing more needs to be said.

Mr. Scholl, you talk about the—how NIST did the introduction to cybersecurity, a bunch of really interesting things that NIST has done. And it says that the introduction has to move to the next big place, which is actual standards. Will NIST develop that? Are they the best people to develop it? And when do we go from just sort of suggesting, here's a way to approach, to actually mandating or laying out the very clear guidance needs that both the commercial and the government sector have to take? When do we move from an introduction to something that's actually real?

Mr. SCHOLL. Yes, thank you for the question. So the intent of the document that we wrote on the introduction was to lay out the process steps that an individual organization will walk through in order to make it real for the technologies that they're using or the type of space operation that they're working under, either purely owned or outsourced or maybe some hybrid, as well as for the context of their business. Now, these all have wide variations and many differences, so our initial document was to introduce how an organization works through that risk management process to develop something that's real and that will be meaningful for their business and their mission to assure what their operations need to secure.

The next steps, then, are to ensure that individual organizations really understand how to implement these processes and then potentially for us to work in an open standards body alongside industry to develop those next step things, so not necessarily NIST, internally, but now externally in a participative standards body alongside industry to grind out the next level of detail.

Chairman BEYER. Thank you, Mr. Scholl.

And, Mr. Bailey, let me pivot on almost—just follow up to that question. You talk about the lack of a binding space cyber policy for commercial space technology, and the Space Directive–5 exists, but it's nonbinding. Can it be—can we get a binding policy, cyber policy, for space for commercial and noncommercial? And is NIST the folks to develop that? Or is it Aerospace?

Mr. BAILEY. Thanks for the question. So I think we can create some binding level of policy to some degree based on—there's probably—there's definitely some minimum standard type of implementation for security that we could look to leverage, and Space Policy Directive–5 actually hints to many of those principles that we would—no one would disagree with that are good and can be binding. But it's—like I said, it's nonbinding, so you can't really force people to do it.

Now a majority of people that are developing these systems, commercial and government, are doing many of the things that are listed in Space Policy Directive–5, but it's not necessarily a requirement. So there are some level—and NIST could be helpful, as well as some of the communities that are popping up within like the space ISAC, for instance, could help drive some of those policy implementation details, as well as aerospace being an FFRDC continue to help and assist with that as well because there definitely are some minimum standard things I think we could get into a policy document.

Chairman BEYER. Great. Thank you very much. Let me now recognize the Ranking Member of the Space Subcommittee, Dr. Brian Babin.

Mr. BABIN. Thank you, Mr. Chairman.

First question to all witnesses—and thank you for being here with us—the Cybersecurity and Infrastructure Security Agency, or CISA, is the primary Federal agency tasked with addressing the cybersecurity of our Nation's critical infrastructure. In May 2021, CISA announced the formation of a Space Systems Critical Infrastructure Working Group to bring together stakeholders from across the whole sector to minimize risk to space systems. And a very—just a short answer if you don't mind. How are each of you working with CISA on this effort? Let's start with Mr. Scholl.

Mr. SCHOLL. Yes, certainly. So I have attended some of those meetings and discussed cybersecurity standards and tools that NIST has that could be applicable to space operations with this working group. But in general, we have an extensive partnership and collaboration with the DHS, the National Risk Management Center (NRMC), mostly through their space weather and space risk organization in the NRMC. So even outside of the work that—this specific working group, we do collaborate and work extensively with DHS, who is focused on this issue.

Mr. BABIN. OK. Mr. Bailey?

Mr. BAILEY. Yes, The Aerospace Corporation is involved in those working groups and meetings, so there is involvement there from The Aerospace Corporation side of the house. I've yet to see necessarily any output from that organization quite yet to understand what their—you know, what the goal will be in the end and how it's going to affect change in the future, but there is involvement with aerospace and that group.

Mr. BABIN. All right. Thank you. And Dr. Suloway?

Dr. SULOWAY. Yes. We're supporting—I am supporting the CISA working group, as well as are the—one of the sub-working groups that is publishing a paper either end of this month or early next month around how to further the work from the NIST profiles that have been published within CISA, so that work is coming. And there's a lot of debate in that working group on the adoption of the critical infrastructure as a sector. So I think—there are reports going to be published in the next few months.

Mr. BABIN. All right, thank you. And, Mr. Scholl, the smaller companies in the space launch industry may not be familiar with the NIST cybersecurity framework, but it's been a sector that NIST has focused on through the National Cybersecurity Center of Excellence, the NCCOE. How is NIST engaging the space sector during the current process to update the new cybersecurity framework 2.0?

Mr. SCHOLL. That's a great question. And so we've done some active and targeted outreach to some of these communities, especially as you said, small space operators, to ensure that we understand and get their feedback on the usability of the framework for their mission areas. And we reach out to both individual companies, as well as through organizations like the Satellite Industry Association, which helps us bring them together into one organization and it also amplifies our message back out to their members as well. The Chamber of Commerce has also been extremely helpful in reaching this community for us as well.

Mr. BABIN. OK. And then again—or once again, there, Mr. Scholl, in May 2021, President Biden signed Executive Order 14028, "Improving the Nation's Cybersecurity." As part of the EO, the Executive order, NIST was tasked with identifying ways to increase the security of software supply chains, which will be incorporated into new Federal Acquisition Regulation (FAR) for Federal contacts moving forward. In a July 2022 update, NIST indicated that it needs to continue to work to review the proposed FAR regulations to ensure they are consistent with the requirements of the

Executive order. What is the status of this work, and when do you expect these FAR regulations to be released? And what's the expected timeline for compliance?

Mr. SCHOLL. Yes, thank you for the question. So NIST has published a series of guidance, recommendations, and tools to improve the the security of our software supply chain. The publication and the update of the Federal Acquisition Regulation or the FAR is not the NIST responsibility within the executive order but rather will be conducted by GSA (General Services Administration), who has oversight on the FAR, and the implementation of that will come down through the Office of Management and Budget in policy directives to the agencies writ large. NIST has built the foundation in the guidance and the directives that will be used by both commercial and government software developers that both the FAR and the policy will cite for those requirements. So we've laid the foundations and the groundwork. Now the organizations that have responsibility for governmentwide policy and for acquisition regulation will be the next step. And those are external to NIST.

Mr. BABIN. OK, thank you very much. My time is expended, so I'll yield back, Mr. Chairman.

Chairman BEYER. Dr. Babin, thank you very much.

Let me now recognize the Member of Congress who will—whose district will oversee the Artemis launch to the Moon in the next 60 days or so, Mr. Posey.

Mr. POSEY. Thank you very much, Mr. Chairman, for holding this hearing.

It seems the threats to our national security never ends. They just get greater and greater, and I thank the panelists for coming today and sharing your thoughts with us.

The vast majority of space technologies are dual use. I mean, they can serve both in national security and a civil purpose. Companies like L3Harris, which is headquartered in my district, offers solutions to protect government systems. Many other companies manufacture, launch, and offer solutions to protect them as well. Are there any barriers that any of you see between the cybersecurity solutions provided for national security civil and commercial space sectors?

Mr. BAILEY. I'll jump in here. So one of the things I see is the barrier for information sharing between government national security and commercial. So there's been numerous times where I've been involved in conversations where they kind of have to stop because the proper caveats or access control and information can't be shared with certain commercial entities for certain reasons. So that leads to not understanding the threat necessarily, as well as maybe national security individuals may have, so that can lead to a misrepresentation, misunderstanding of what kind of threat they're actually trying to mitigate. So there definitely needs to be some breaking down the barriers there, getting some information sharing at the highest levels to individuals who need it so that the engineers and implementers that are actually doing the system engineering need the information.

Mr. POSEY. Do you see that there is a potential solution to the problem?

Mr. BAILEY. Yes, there's—there could be. Getting sponsoring access to certain contractors that build these solutions or temporary, you know, clearances for individuals, which they've done that in the past at certain levels, like getting, you know, read on the certain accesses for a certain meeting or something like that, so opening up that information flow. But I think one barrier—one avenue that could potentially help is with the standup in the last couple of years with the space ISAC. There could be—that could be an avenue to get information distributed out to a wider community who are members of that community. However, it has to be kind to—have to be certain—you know, certain things have to be done with the information to make it shareable. And that needs—work needs to be done, you know. So having someone to handle that part to get the information, declassified or demarked down to a certain level that can be shared will be critical.

Mr. POSEY. Great—that's a great answer. Again, to anyone on the panel, how are you working with the aerospace and defense sector to ensure government use applications have cyber protections built into the requirements?

Dr. SULOWAY. So I actually have an answer to the previous question on barriers for DOD on civil and commercial. In my view, the DOD and civil agencies which have requirements are able to fund the—or the addition of security measures to their satellites. But for commercial vendors, they are driven by the consumers of the services that are being used, and so they may not be as willing to pay for security as a DOD or a civil agency would because they're required to do so. So I think it's important to remember that commercial—solely commercial entities won't have the ability to be competitive with other entities that don't include security if that's not somehow incentivized by the government to do so.

Mr. POSEY. That makes perfect sense. Do you see solutions to that?

Dr. SULOWAY. I think when it comes to cybersecurity, the NCCOE has been able to help private industry adopt cybersecurity without a lot of additional costs by developing practice guides that show commercial entities that do the R&D to integrate security tools into a reference architecture to help kind of lower that entry into using commercial—commercially available cybersecurity products. And so I think similar R&D and guides that can help commercial space—the commercial space community adopt without having to do a lot of experimentation to implement cybersecurity tools would be helpful. So guides and additional references would help.

Mr. POSEY. I see my time is expired. Thank you, Mr. Chairman. I yield back.

Chairman BEYER. Thank you, Mr. Posey.

Let me now introduce the Chair of the House Administration Committee, Ms. Lofgren.

Ms. LOFGREN. Well, thank you very much, Mr. Chairman, and all the Members of the Committee. I think this is an extremely important hearing, and I'm grateful that we have organized it.

You know, when you think about the space sector, the commercial side may not have the same protections that we have in the governmental side. And yet, a cyber attack could be simply devastating to the American economy and to the world economy, so this is hugely important. I'm wondering, especially since it looks like we will be taking up the *CHIPS Act* today, we know in other sectors that supply chains and third-party vendors can present significant cybersecurity vulnerabilities. So how much do we need to worry in space systems' supply chains posing cybersecurity risks, and what should we do about it? I mean, one of the concerns that's been raised publicly, I won't get into any of our classified briefings, but Huawei's vulnerability is some—well-known or has been publicly discussed. We hope to overcome that through the the *CHIPS Act*. Can any of you address that?

Dr. SULOWAY. So at least from my perspective, cybersecurity—the supply chain risks that you would have in space systems, as you would in any other industry, are going to be there, and there are a few things you can do. But I think monitoring your systems because you are not going to be able to fully vet every single line of code that you could be bringing into your environment. So again, monitoring and sharing information, as Mr. Bailey mentioned earlier, is important to do for the commercial space industry in general, especially because—especially for space systems, it's harder to deal with things when—once systems are in orbit, so monitoring is really important.

Ms. LOFGREN. Correct.

Mr. SCHOLL. I'm——

Ms. LOFGREN. Go ahead.

Mr. SCHOLL. I'm sorry, if I may. Yes, information security—information supply chain risk management is a hugely important field, which has shown itself even more so after the Log4j vulnerability issue and SolarWinds. And so there's been a significant focus that can and should be applied to the supply chain and commercial satellites as well.

This technology, though, has the potential to be monitored and managed a little tighter just because of the desire and the need for technologies that have a space pedigree. This is not necessarily a technology space that's as wide as commercial off-the-shelf technologies that are used in our IT systems. It's a smaller set. They have to survive the violence of launch and the environments of space. So people look for technologies that are specialized for that. So there's an opportunity here to understand and provide visibility into a supply chain.

Mr. BAILEY. I can say one thing real quick. So I agree with what Mr. Scholl said. However, on the commercialization of space that we're seeing and the influx is you are starting to see a little more commoditized standard technology that's being used, and open source software that's being used that we haven't seen in the past. So I think the supply chain aspect is going to be of increasing importance with the commercialization of space because now you're seeing entities run like real-time Linux on spacecraft where before you would never see that. And then you have the ASIC (application-specific integrated circuit), FPGA (field programmable gate array) hardware-based Trojan things that can happen if you offshore those and don't have those under a good lock and key so that—it's going to be increased importance for sure.

Ms. LOFGREN. I thank all of the witnesses, Mr. Chairman, and I yield back.

Chairman BEYER. Ms. Lofgren, thank you so very much.

We're now going to do a second round of questions for those Members who would wish to do so. And let me begin.

Dr. Suloway, you had mentioned—I think Mr. Bailey mentioned also—that designating space systems as a critical infrastructure sector within DHS, that there are 16 existing already. My—our good friend, Congressman Ted Lieu from California, actually introduced legislation specifically to do that, which has not yet passed. Is this the right way to go? And how big a priority should this be for us?

Dr. SULOWAY. There are several aspects to having space as a critical infrastructure, and I think the advantages of having it as a—space as a critical infrastructure allows there to be a focus location for commercial entities to kind of engage with the Federal Government. I know there is also a lot of concern that it would add additional burden to the commercial space industry, and that's why some people are concerned about bringing it as an additional sector. And so I think whatever is done, a centralized focus is important, and the implementation of it needs to be done carefully so that it doesn't have the opposite effect of driving commercial entities to not work within the United States and register abroad. And so I think that's my only concern.

Chairman BEYER. You led very nicely into the second question. Of the three recommendations you made, the first one was that we incentivize adoption of best practices rather than regulate them. Is this the same concern that they would locate in other countries if we regulated?

Dr. SULOWAY. Yes, that's the main concern is that we want them to be part of the conversation. And as Brandon mentioned, from a space information sharing perspective, we want them to bring their data into the fold so that the community itself can get stronger. But if commercial entities who have to serve customers aren't able to be profitable with adding in additional requirements, that's an issue. I will say the space community, at least the ones that participate with the ISAC, are very motivated to be involved and are applying their resources, so I just want to protect that community and with whatever is done from a critical infrastructure perspective.

Chairman BEYER. Mr. Bailey, let me pile on because this is a constant debate here is how light, how heavy should the regulatory touch be. So if we're in a place where we're encouraging based on NIST recommendations and not mandating, not having a set policy, what's the danger of the bad actors slipping through in some five percent, 10 percent, 20 percent of the cases? How do we find that right balance?

Mr. BAILEY. Yes, I think incentivizing is one mechanism. Maybe there's a balance between minimum—a minimum implantation standard like encryption or other—or maybe some supply chain controls as minimum and then incentivize to increase maybe additional levels of security. And it's not a one-size-fits-all either. It's not every single satellite that gets launched needs needs a certain level of security. It's a risk-based decision. And so anything that's being leveraged to provide critical functionality for the country should meet, you know, these minimum standards, but maybe, you know, a small research CubeSats or nanosats that are running for universities may not have to be the same level of security. So it's going to have to be a risk-based decision. And as these things get used for critical functions in the country, I think the barrier and the minimum standard has to be established because, I mean, at a minimum, what we've already—I mean, encryption is super important. I think we all agree that should be done. And the fact that we don't have that as a binding requirement for any satellite that's launched in this country is a little concerning from my perspective.

Chairman BEYER. Great. Great. Thank you very much.

Dr. Scholl, you talked about formalizing and strengthening the government's relationship with Space ISAC. Tell us a bit more about Space ISAC. Is it governmental, quasi-governmental, private?

Dr. SULOWAY. It's a private company, but they are—they do have relationship with DHS, so they're chartered by—I think they have a relationship of information sharing with with DHS. But right now, they don't have a formal Federal Government role, and I think that's where the—there can be confusion from a commercial space perspective of where—if they wanted information, where do they plug in? Do they go to the FBI or do they go to DHS or, you know, should they participate with the space ISAC? It's—I think it would help to formalize that relationship so commercial companies could feel comfortable providing that information and know that they were plugging into the appropriate part of the ecosystem because there isn't a central, I think, location to go to.

Chairman BEYER. OK. Thank you. If if Dr. Babin is here—I don't believe he is. But, Dr. Babin, if you're here, we'd love to welcome you for a second round of questions.

So moving on, let me—Dr. Suloway, let me also just follow up on that. ISAC—Space ISAC is it nonprofit?

Dr. SULOWAY. I believe it is a nonprofit, but I do not know that off the top of my head. I would have to get back to you.

Chairman BEYER. And how would the government formalize this relationship with ISAC?

Dr. SULOWAY. So that is a good question. I am not as familiar with how the Federal Government formalizes relationships with ISAC, and so I would have to get back with you on what the specific mechanism would be for that.

Chairman BEYER. Mr. Bailey, if I could just pivot on this same question, you talked about a proper sector-specific agency, SSA, a sector risk management agency working with something like ISAC. Is this something, again, that's created from scratch based on an earlier model or does it already exist?

Mr. BAILEY. Well, the real intent of that comment was ensuring that we select the proper, you know, sector agency and not affiliated with maybe agencies who aren't necessarily or can't tap into the space domain knowledge that does exist in the Federal space. Because currently we have—you know, between NASA, you know, Space Force, NRO (National Reconnaissance Office), NOAA, we have numerous agencies, professionals, and people who understand this domain and understand cybersecurity concerns and the nuance thereof. So the real crux of that comment is really ensuring that we leverage those agencies in addition to the community that the ISAC is building with the commercial sector to implement that properly. So what you don't want is, you know, necessarily some bureaucratic agency that has little domain awareness that relegates a whole bunch of red tape that just stifles innovation.

So that's really the goal is making sure that you have the proper bounds of oversight with people who have domain expertise and then working directly with entities like the ISAC to the further the, you know, cybersecurity posture and prove it across the board. So if we were to do the critical sector, critical—space technology is a critical infrastructure sector. Whoever that, you know, agency is, that's probably where you could have that tie-in with the ISAC and have that kind of point-to-point communication in my opinion.

Chairman BEYER. Great. Thank you, Mr. Bailey, very much.

Let me yield to my good friend, the Ranking Member, Dr. Babin, for his questions. In the meantime, Congresswoman Kim will follow Dr. Babin.

Mr. BABIN. Thank you very much. I wasn't quick enough getting audio back on. I'm sorry, Mr. Chairman.

Yes, I do have a couple more questions, this one to Dr. Suloway. How does MITRE support small- and medium-sized businesses in the space industry on cybersecurity standards and best practices? And how does MITRE work to explain what the attack framework is to the commercial space industry?

Dr. SULOWAY. So MITRE works with several industry associations like AIAA (American Institute of Aeronautics and Astronautics) and engages with them on that front. As far as MITRE ATT&CK, there isn't a specific MITRE ATT&CK for space systems. But we do provide the MITRE ATT&CK framework because—generally to all. So we are engaging heavily in forums and conferences with the commercial space community, which is actually where we've heard a lot of the concerns from a regulatory perspective. And so those are the engagements we've had.

And yes, MITRE ATT&CK is helpful, but it's important to remember that MITRE ATT&CK is based on tactics, techniques, and procedures that have been observed in other systems. And there hasn't—you guys have mentioned several of the incidents that have occurred for space systems, but there isn't that large body of knowledge as there are with traditional network systems, and so there's a lot of, I guess, predictive nature of looking at a tech and how it could apply to space systems because there isn't that knowledge base.

Mr. BABIN. All right, thank you. Thank you so much. And one more, Mr. Chairman, if you don't mind. This is addressed to Mr. Bailey. Information Sharing and Analysis Centers, or ISACs, are forums for private sector information sharing related to critical infrastructure and cybersecurity. According to the National Council of ISACs, they are typically nonprofit organizations which do not lobby. I think you all mentioned that a second ago. A new ISAC focused on space was recently established, and both aerospace and MITRE are members. Is the space ISAC a nonprofit or—and does it advocate for policy positions?

Mr. BAILEY. I also don't know 100 percent for sure if it is nonprofit, but I believe that is the case, given the—how ISACs operate. And yes, Aerospace and MITRE—and we support the ISAC. And we don't really lobby for anything. We've necessarily put out what we feel like is the appropriate, you know, guidance or position that the ISAC would want to have as it relates to cybersecurity.

So one of the things that we've done in the ISAC community that we're currently working on—we haven't published anything yet—but is trying to translate Space Policy Directive–5 from a policy, even though it's nonbinding, to implementation details that can actually be shared in the community. So that's an ongoing effort. There's a Space Policy Directive–5 working group where we're trying to better articulate some implementation technical guidance as it relates to the principles that were outlined in SPD–5. So that's kind of where—we're more in the nuts-and-bolts area of this, but there is some——

Mr. BABIN. Yes.

Mr. BAILEY [continuing]. Policy aspect to that.

Mr. BABIN. OK.

Mr. BAILEY. And if I may, if I could answer your—the question you had before——

Mr. BABIN. Sure, go ahead.

Mr. BAILEY [continuing]. So the question you asked before about how MITRE supports—Aerospace does similar activities with—our focus is space. So MITRE does a lot of their work, great work with ATT&CK and other things. Aerospace is really focused mostly on space systems. And the way we collaborate with industry and things is like we published that technical operating report this year with a coordination through a government agency to get it in the public sector so that can be shared to commercial entities on the threats that could apply to a spacecraft, as well as countermeasures and ways to implement those and even get those into acquisition requirements and design details. So we're trying to put out additional low level guidance that can help mitigate some of the cyber attack threats that we see that could manifest itself onboard a vehicle. And we also have initiatives ongoing that kind—that try to leverage what the MITRE ATT&CK framework is but kind of translate that for what it would really mean to a space vehicle. And we're—we have ongoing research in that area. Thank you.

Mr. BABIN. OK, thank you. Thank you so much. Excellent.

Mr. Chairman, I yield back, and I appreciate the second round.

Chairman BEYER. Thank you, Mr. Babin, very much.

Let me now recognize the gentlelady from California, Mr. Kim—Ms. Kim.

Ms. KIM. Thank you, Chairman Beyer and Ranking Member Babin, for holding this hearing today. And I do appreciate the opportunity to ask our witnesses questions in the second round.

Space already plays a very integral part in our lives, and with the commercial space boom, we have witnessed in recent years we should expect that our lives will be increasingly reliant on technology in Earth's orbit. This means we'll be increasingly reliant on cybersecurity. So I can ask this question to either Dr. Suloway or Dr. Scholl. In your written testimony, Dr. Scholl, you noted that examples of malicious cyber activities harmful to space operations include spoofing sensor data, corrupting sensor systems, jamming, or sending unauthorized commands for guidance and control, injecting malicious code, and conducting denial-of-service attacks. This is what you said Mr.—Dr.—Mr. Scholl. So based on your experience of working with the private sector to implement Space Policy Directive–5, would you say maligned state actors are the greatest threat to America's commercial space industry?

Mr. SCHOLL. So, yes, thank you for the question. Nation-state actors are one of the most resourced and motivated to disrupt this infrastructure of the threat actors that exist. So certainly a nation-state actor has the resources, has the capability, and has the need from a competitive perspective as a threat actor that we should be prioritizing.

Ms. KIM. Sure.

Mr. SCHOLL. A lot of these attacks are described, absent of the actual threat actor. A tier down is the potential authorized and—person who has access but for whom there's an accidental input, a disruption, an interference with an adjacent band. So, yes, nation-state actors first, but there's also a whole other class of threat actors, which are known as the accidental but authorized as well.

Ms. KIM. Sure. For the past year, our Committee has worked on legislation to increase the number of graduates entering STEM (science, technology, engineering, and mathematics) fields, including cybersecurity. So I want to ask you, Dr. Suloway, what is your assessment of the cybersecurity work force in the space industry and in the Federal Government's space agencies?

Dr. SULOWAY. So it is a challenge to find individuals with both a space background and a cyber background. And I think, just anecdotally, it is hard to get both of those backgrounds together in a single person. So more investment in education would be—which would be helpful.

Ms. KIM. Dr. Suloway, are you aware of any state-sponsored cyber attacks on American commercial space companies? And if so, what was the damage that you're aware of?

Dr. SULOWAY. So I can speak to the two recent events that Chairman Beyer brought up in his testimony, which were the SpaceX terminals in Ukraine, as well as the Viasat. So from a Viasat perspective, it's interesting because the attackers were able to get in from the ground system and then move to the user terminals and then disable those systems. So it's interesting from a ground user space, getting into one allows you to pivot to the other. In that case, they disabled the terminals, which were able to be recovered at a later state but disrupted the service. So it was recoverable, but I don't know the full impact of what wasn't able to be done without that service.

Ms. KIM. So I know the last question you asked you responded, and I wanted to just see what kind of attacks that you're aware of, and if so—but I do agree with you that we lack work force in the STEM-related fields. And I think that is the more reason why our government has to invest more in educating the next generation of future scientists, future—you know, the work force in the STEM field. So I know I'm working on legislation collectively with my colleagues, one of which was already included in the CHIPS legislation that we're working on this week. So I really agree that we need to build our work force in that development, and I'm really using this time to encourage my colleagues to think through it as we vote on that legislation today. Thank you.

Chairman BEYER. Congresswoman Kim, thank you very much for coming and being part of this.

Before we bring the hearing to a close, I really want to thank our witnesses for your testimony. As I understand, there are roughly 4,500 satellites in low-Earth orbit today. They project 100,000 by the year 2030, which is not far away. We're depending on them for communications, for weather, for agriculture, for national security, and probably most importantly for the internet for the whole world. And it's critical for life in the 21st century that we protect the satellites and the ground-to-satellite, satellite-to-ground communications.

So this a really important hearing. Thank you so much for all of your input. Thanks for the ideas and the wisdom. We will try to figure out a way forward with your help.

The record will remain open for two weeks for additional statements from Members and for any additional questions the Committee may ask of the witnesses. The witnesses are now excused. The hearing is now adjourned.

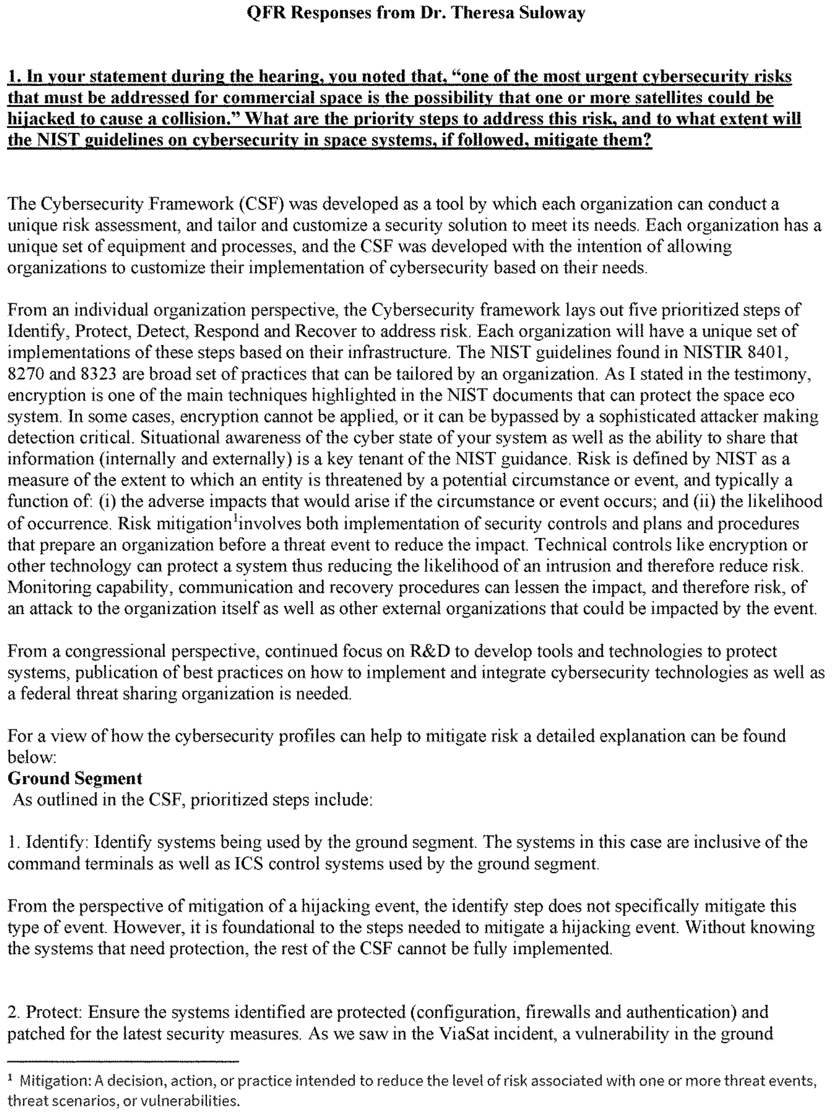
[Whereupon, at 11:17 a.m., the Subcommittee was adjourned]

Appendix

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Theresa Suloway



QFR Responses from Dr. Theresa Suloway

1. In your statement during the hearing, you noted that, "one of the most urgent cybersecurity risks that must be addressed for commercial space is the possibility that one or more satellites could be hijacked to cause a collision." What are the priority steps to address this risk, and to what extent will the NIST guidelines on cybersecurity in space systems, if followed, mitigate them?

The Cybersecurity Framework (CSF) was developed as a tool by which each organization can conduct a unique risk assessment, and tailor and customize a security solution to meet its needs. Each organization has a unique set of equipment and processes, and the CSF was developed with the intention of allowing organizations to customize their implementation of cybersecurity based on their needs.

From an individual organization perspective, the Cybersecurity framework lays out five prioritized steps of Identify, Protect, Detect, Respond and Recover to address risk. Each organization will have a unique set of implementations of these steps based on their infrastructure. The NIST guidelines found in NISTIR 8401, 8270 and 8323 are broad set of practices that can be tailored by an organization. As I stated in the testimony, encryption is one of the main techniques highlighted in the NIST documents that can protect the space eco system. In some cases, encryption cannot be applied, or it can be bypassed by a sophisticated attacker making detection critical. Situational awareness of the cyber state of your system as well as the ability to share that information (internally and externally) is a key tenant of the NIST guidance. Risk is defined by NIST as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Risk mitigation[1]involves both implementation of security controls and plans and procedures that prepare an organization before a threat event to reduce the impact. Technical controls like encryption or other technology can protect a system thus reducing the likelihood of an intrusion and therefore reduce risk. Monitoring capability, communication and recovery procedures can lessen the impact, and therefore risk, of an attack to the organization itself as well as other external organizations that could be impacted by the event.

From a congressional perspective, continued focus on R&D to develop tools and technologies to protect systems, publication of best practices on how to implement and integrate cybersecurity technologies as well as a federal threat sharing organization is needed.

For a view of how the cybersecurity profiles can help to mitigate risk a detailed explanation can be found below:

Ground Segment

As outlined in the CSF, prioritized steps include:

1. Identify: Identify systems being used by the ground segment. The systems in this case are inclusive of the command terminals as well as ICS control systems used by the ground segment.

From the perspective of mitigation of a hijacking event, the identify step does not specifically mitigate this type of event. However, it is foundational to the steps needed to mitigate a hijacking event. Without knowing the systems that need protection, the rest of the CSF cannot be fully implemented.

2. Protect: Ensure the systems identified are protected (configuration, firewalls and authentication) and patched for the latest security measures. As we saw in the ViaSat incident, a vulnerability in the ground

[1] Mitigation: A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.

segment was used to gain access to the user segment, which was then used to disable user terminals. Similarly, attacks on the ground segment could be used to cause harm to the space segment.
This step could have prevented the ViaSat attack and if properly implemented will reduce the likelihood of a command link intrusion.

From the perspective of mitigation of a hijacking event, the protection of the command-and-control infrastructure is critical. As we note in the following paragraphs, some space vehicles have little to no protection against cyber-attacks and will trust commands from the ground. A malicious set of commands sent from the ground will be accepted by the vehicle and executed.

3. Detect: An out-of-band monitoring system is a tool that can be used to detect bad actors able to move past the protections that have been applied to given system. Out-of-band systems provide for communication channels separate from the systems that may be attacked or exploited. Out-of-band monitoring systems can be costly to implement, but offer an important part of a defensive strategy against cyber-attacks. Because a protection system is unlikely to be perfect, a detection system is important to identify attackers in a system. If a detect mechanism had been in place with ViaSat, the operators might have seen the behaviors of the attackers moving throughout the systems to gain further access to the network.

From the perspective of mitigation of a hijacking event, the timely detection of a malicious actor in the ground control infrastructure can allow ground operators to remove that actor from the control systems before it can send malicious commands to the space system. Automated tools that provide operators with information quickly can mitigate a hijacking event.

4. Respond: The NIST CSF and NISTIR 8401 outline the types of procedures, processes, communication plans and automated tools that organizations should document and on which their employees should be trained in the case of a cyber incident. Communication within the targeted organization, as well as communication with external parties, will help other organizations that might be affected peripherally by an attack to assess their risk and take mitigation actions if necessary. The use of automated response tools can help to contain and mitigate the impact of a cyber incident. The speed at which a cyber incident is contained and mitigated is important to space systems. A capability such as security orchestration automated response (SOAR) can help mitigate the extent of damage a cyber attack can achieve. “Failing over” to alternate systems or other ground infrastructure is also a mitigation option that can be used to limit the impact of a cyber-attack.

From the perspective of mitigation of a hijacking event, the ability of a ground segment operator to respond quickly to a hijacking event is critical. Even as a spacecraft is being operated by a malicious actor. the ability to communicate quickly with other organizations to alert other space operators of a problem will help to maneuver other vehicles out of harm’s way and avoid a collision. Having procedures in place to fail over or disable the current infrastructure can also prevent the attacker from continuing to control the satellite system.

5. Recover: The recovery step involves processes, procedures, and tools to restore the original system to a trusted state. Automated tools to conduct validation can help to speed the recovery and restore services. Mitigation techniques should also be communicated to other organizations to ensure others are able to take action to protect their systems.

From the perspective of mitigation of a hijacking event, there is a period when an attacker is in the defeated initial protection system but is moving laterally within the system to gain additional access to achieve control. A robust monitoring system potentially can detect these activities. The ability to remove the attacker quickly and prevent them from sending commands to a satellite can prevent a hijacking event. The CSF has informative references on how to implement recovery processes and procedures.

Space Segment

Space systems are limited in Size, Weight, and Power (SWaP). Space systems use Real Time Operating Systems that are not as widely used as commercial operating systems. Space Systems use protection mechanisms that are unique (and often legacy) software. For cyber, "one off" software does not leverage modern best SW design practices, nor does it benefit from community wide examination and scrutiny. Also, the longer software is available, the longer an attacker has time to find a vulnerability. There isn't a developed market for cybersecurity products for space systems. Typically, the only security used by a space system is encryption to secure the link to the ground. If the encryption is not used or bypassed via a compromise on the ground segment, then there is little to no protection.

1. Identify: This step is relatively easy for a space system because all the assets are contained within the vehicle.

From a hijack mitigation perspective this does not prevent an attack but is foundational for the other steps of the CSF.

2. Protect: The primary protection for the space system is to only accept commands from a trusted source. This typically involves encryption of the commands. Geostationary orbit satellites that are continually in view of their ground station may utilize signal power, timers, or message counters to validate commands or prevent other entities from transmitting to the satellite. These methods do not provide the same security as encryption but may be implemented by companies and offer minimal protection.

From a hijack mitigation perspective, protection of the command link to the ground can prevent or mitigate hijacking from a malicious source on the ground. If the ground segment is compromised, sending commands through the "trusted" encryption system will not protect the system.

3. Detect: There are no systems that currently provide a detect function for commercial space vehicles, although the Space Information Sharing and Analysis Center (ISAC) is putting in place an architecture to detect anomalous behavior that may be the result of adversary activity. Most detection is done from the ground through the analysis of telemetry; cyber-related data, including data indicative of anomalous behavior, is not typically conveyed from satellites to the ground. The identification of the proper data elements that are needed to perform the analysis is an open research topic.

From a hijack mitigation perspective, an on-board detection capability that could operate autonomously, without assistance from the ground, could prevent malicious commands from being executed on the vehicle even if the ground segment were to be compromised.

4. Respond: The response capabilities of a space system would be driven largely by the ground because the space segment does not typically have an internal cyber detection system (also known as an intrusion detection system, or IDS). Relevant data would need to be sent to the ground and analyzed, and then commands to respond would need to be sent back to the space system. In the future, mechanisms that could conduct these activities on the space segment are needed.

From a hijack mitigation perspective, an autonomous respond-on-board capability, coupled with an on-board response capability, could quickly reject anomalous commands and protect the system from further malicious manipulation.

5. Recover: The space segment must have an on-board capability to recover to a trusted state. The ability to validate and test the trustworthiness of the system to reestablish a trusted link with a trusted ground station is important.

From a hijacking mitigation perspective, the ability to return to a trusted state after a hijacking attack or attempt is critical for the space segment to return to providing services.

2. To what extent do cybersecurity risks and threats differ across civil government agencies and commercial space systems? a. How are the approaches to managing cybersecurity risks for civil government space systems similar or different to those for commercial space systems?

Answer: The threats to civil and commercial systems are the same and have been published (Figure 1) by the National Air and Space Intelligence Center (NASIC). NASIC calls out the Link Segment as a separate segment. NIST has chosen to incorporate the link segment into the ground and space segment.

The risks differ for civil versus commercial space systems. The table below categorizes the threat actors and how that translates to risk. Risk is defined as a measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST-SP800-37r2]. In my assessment the risk to commercial is greater due to the "soft target" nature of commercial space. The tool set to access these systems from a ground perspective already exists and can be used against an unprotected or minimally protected system, versus a civil system which is FISMA complaint.

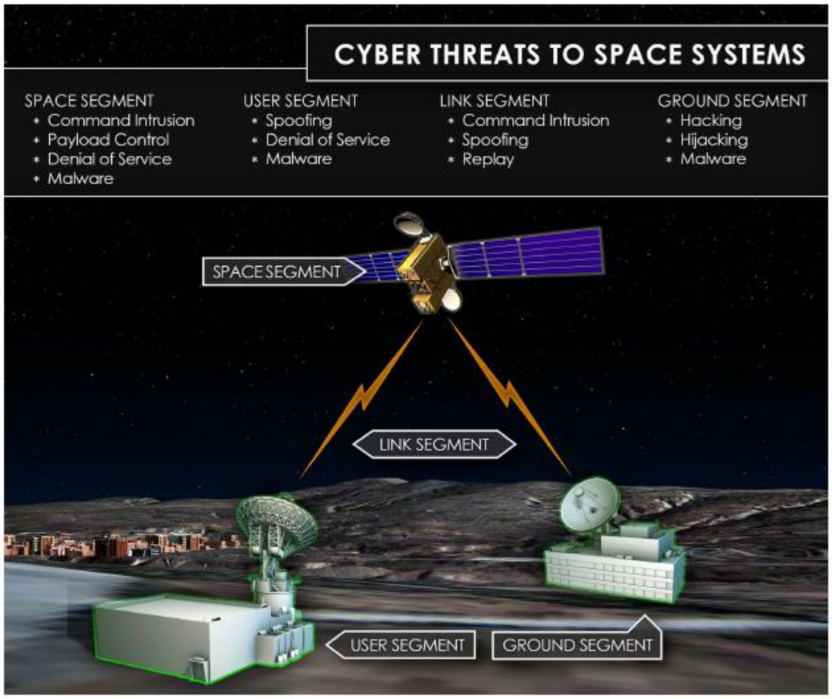


Figure 1. Threats to Space Systems as Published by NASIC[2]

[2] NASIC, Competing in Space, 190115-F-NV711-0002.PDF (defense.gov)

Table 1. Risks to civil vs commercial

Attacker type	Risk to civil operated systems	Risk to commercial (LEO, maneuverable)
Nation-State	Impact: High-- loss of mission, loss of asset or life if a collision occurs, potential conflict with US if attack is attributed Likelihood: Low--the consequences of an attack could lead to conflict between nations and because of the strong cybersecurity measures that are in place for civil systems Risk: Low	Impact: High--loss of service, loss of profit, loss of assets or life, liability if collision with US asset or loss of life occurs Likelihood: High--commercial space is a “soft target” with less protection, and because nation-states do not suffer the same repercussions as attacking a US target Risk: High
Organized criminal/ Terrorist organization	Impact: High--loss of mission, loss of asset or life if a collision occurs Likelihood: Low--less likely due to the cost and technical knowledge needed to perform a successful attack Risk: Low	Impact: High--loss of service, loss of profit and assets Likelihood: High--can provide a global impact for a small investment; can use ransomware and other techniques to extort money from operators Risk: High
Individual activist	Impact: High--loss of mission, loss of asset or life if a collision occurs Likelihood: Low due to skills needed to gain access when the system has implemented FISMA Risk: Low	Impact: High--loss of mission, loss of asset or life if a collision occurs Likelihood: High--can provide a global impact for a small investment[3], Risk: High
Insider threat/ Influence	Impact: High--loss of mission, loss of asset or life if a collision occurs Likelihood: Low--civil operators are US employees and subject to increased vetting processes Risk: Low	Impact: High--loss of mission, loss of asset or life if a collision occurs Likelihood: High--operators not vetted to the same degree as civil systems Risk: High

The approaches to managing cybersecurity risk for civil versus commercial are driven by consumers and what they are willing to pay for, and by investors and the effects these approaches have on their investments' performance. The civil government consumer is willing generally to pay for security and therefore will provide requirements and funding to implement security controls. Also, the civil government community is bound to follow FISMA, which dictates use of 800-53 controls. The commercial industry is driven by the private consumer, who is looking for low-cost service, and by investors seeking acceptable financial performance.

[3] https://threatpost.com/black-hat-satellite-comms-eavesdropping-hack/158146/. Note: while this was a breach in the confidentiality of the satellite telemetry it would not have resulted in a mission loss. However similar techniques could be leveraged for a more serious impact.

b. How do the cybersecurity risks for civil and commercial space systems differ from those of national security space systems?

The commercial space industry is generally at higher risk because it presents a "soft target" to most attacker types, and tools exist to attack the systems that satellite systems rely on. Commercial satellites can be accessed remotely if a commercial operator is not using an air-gapped ground segment. Commercial satellites with a maneuver capability are at a higher risk, whereas non-maneuverable satellites are at lower risk. Commercial satellites in low Earth orbit are at higher risk than those in geostationary or geosynchronous orbit because the ground station does not maintain constant contact with a low Earth orbit satellite but does maintain contact with a geostationary satellite.

Commercial systems are expanding swiftly, resulting in active surfaces (of devices and users) that are expanding swiftly as well. Commercial systems may rely on commoditized supply chains over which visibility may be more difficult to establish and the security of which may be more difficult to ensure. The commoditization of ground station operations for commercial space systems highlights the need to expand our cybersecurity efforts to a broader set of business sectors involved in the space industry.

c. To what extent are government agencies with experience in civil and commercial space sharing cybersecurity best practices or lessons learned?

We are encouraged by the work of the National Institute for Standards and Technology to publish controls and guidelines for space systems, given NIST's traditional emphasis on supporting adoption by industry of useful standards and best practices. NASA, NOAA, and the Department of Defense possess impressive engineering capabilities and lessons learned; some alumni of these organizations have migrated to commercial space industry and are sharing the benefits of their experience. However, no organized and deliberate effort has yet been developed to share these best practices on a systematic basis.

3. In your oral statement you said that, "Adding encryption to the ground space link would mitigate some of the vulnerabilities," and, "If only one requirement is applied, ensure that it is encryption." a. What is the status of encrypting the ground space link for on-orbit or planned systems?

The answer depends on the orbit and size and customer of the commercial space system. While not a comprehensive review, these are a few examples:

Some commercial companies do not choose to add cryptography if the satellite remains in geostationary orbit. This means that the satellites do not move in the sky relative to the ground station. These satellites typically provide services like broadcast TV and are purely used for non-critical functions. In those cases, companies use very large antennas to transmit to the satellite and use a very small "beam width." Beam width is defined as the area on the ground in which the satellite's antenna has the strongest signal. This means an attacker would have to transmit to the satellite near the true satellite facility to make a link to the satellite. The physical satellite dish that would need to be used to overcome the power of the signal from the correct ground station would be visible from the true ground station and then other mitigation actions could be taken.

Another reason commercial companies do not like to use encryption is that if a cryptographic unit fails, it is another branch of a fault tree that must be investigated if an anomaly occurs on the spacecraft. Typically, when investigating an anomaly on the spacecraft, a detailed analysis of the incident is conducted to determine the cause. A cryptographic unit that is malfunctioning could prevent legitimate diagnostic commands from being executed from the ground to find and fix an issue with the system. A bypass capability is useful but can also be leveraged by an attacker if they are aware of the bypass.

Universities and other small commercial companies that operate non-maneuverable satellites such as cubesats without any propellant on board may elect not to use encryption, because even if an attacker gained access to the system, the satellite could not be maneuvered and cause damage.

In the case where a satellite may be used for a DoD or civil customer, the physical encryption unit will be launched on the vehicle but not turned on until a DoD or civil customer requests the service. Otherwise, the cryptographic unit remains present but turned off.

In the case of future low Earth constellations designed to operate as a mesh network, these systems do plan to use encryption, because the satellites themselves are not always in view of a ground station. During such periods, another ground transmitter could transmit to the satellite and the ground operator would not have knowledge of that event until reestablishing a link to the satellite.

b. How far along is the commercial space industry's understanding of and use of encryption for the ground space link? Is it in the early stages or does industry have a mature understanding of this tool?

The space industry typically has personnel who have used DoD systems and therefore are aware of the process of adding a cryptographic unit to the satellites. The US commercial industry understands how to use the tool, but foreign companies may not be as familiar if they do not utilize US personnel familiar with DoD systems. Some companies carry encryption but do not turn it on because it eats into processing power. Some companies implement encryption but it is not certified by NIST as FIPS 140 complaint. Where the industry is finding new issues is in the provisioning of a key management system that supports a satellite mesh network. In the new mesh networks of the future, a trust relationship needs to be established across the satellite mesh network and this is a new challenge for satellite operators.

c. Are there any issues in applying encryption to legacy systems on-orbit?

Typically, encryption involves the prelaunch addition of an encryption device on the satellite, along with a set of cryptographic keys to be used over the lifetime of the satellite.

Software encryption can be added to a satellite once on orbit if the satellite computational capabilities are able to support it. Increased computational capabilities require more power and therefore there is also a power constraint that must be met. Once the software is in place, a key must be exchanged over RF without being intercepted. The ground must also add in encryption and key management to support the on-orbit changes and maintain a secure link. Legacy systems may not be able to support the computational or power requirement of encryption. Recently, SpaceX was able to encrypt its Starlink telemetry after launch, showing that larger, capable systems can add encryption after launch. SpaceX was able to do this because Starlink firmware can be updated after launch. This capability may not be present on other systems.

4. Many new commercial space systems are deploying as large "satellite constellations," consisting of tens, hundreds, or even thousands of small satellites operating together. To what extent are there unique cybersecurity risks for large satellite constellations as compared to single satellite operations? a. Are there also unique or special risk mitigation strategies to address those risks, and if so, what are they?

Satellite constellation designers have a vision of adding and removing satellites from the "network" to allow for upgrades and resilience of the constellation. A unique requirement of this new architecture when it comes to cyber is the revocation of trust with a satellite that has been compromised by a cyber-attack. Satellites in a mesh must be capable of receiving and responding to an alert regarding a loss of trust when a satellite in the mesh is compromised.

Large commercial space systems will likely have expanded attack surfaces (from many users and connected devices) and a broader supply chain than in small satellite systems and constellations. A larger attack surface will require secure architecture, including possibly zero trust architecture, that mitigate the risks associated with an expanded access to these systems. Effort, including those underway at the Space ISAC, to help the space systems industry gain the best possible visibility into their supply chains can help reduce the likelihood that counterfeit or compromised hardware and software can become part of the technology eco-system that comprise these new constellations. Companies providing ground-station-as-a-service capabilities can employ zero trust approaches, and employ trusted cloud approaches as described by the National Cybersecurity Center of Excellence at NIST. It should also be noted, however, that larger constellations, some of which may have redundant capabilities may be more difficult to attack effectively and could convey stronger resilience to the infrastructures and missions they serve.

5. How does the growing participation of international entities in space affect cybersecurity risks, and to what extent is space cybersecurity addressed on an international level? a. What body, in your view, is most appropriate for international coordination on space cybersecurity?

b. What can the U.S. do to ensure that it leads the way in the development of standards and norms for cybersecurity in space systems internationally?

Growing international participation represents both risks to and opportunities for the cybersecurity of space systems. Other countries, including our competitors and adversaries see our dependence on space systems as potentially exploitable, and are building capabilities requisite to attacking or degrading our space systems' capabilities. These countries may also be less sensitive to the needs for effective space traffic management; Russia's test in 2021 of an anti-satellite weapon, created a cloud of potentially dangerous debris. However, international cooperation with our allies and partners can lead to shared efforts and recognized best practices to strengthen the cybersecurity of space systems; work with DLR, JAXA, and the European Space Agency can provide the opportunity to build stronger, intrinsic cybersecurity into the many systems on which the US, and its allies and partners depend. Indeed, the Space ISAC is building information sharing and supply chain risk management initiatives with international partners, helping extend to our commercial space systems the benefits of cooperative research, development, and engineering.

The United States remains well positioned to develop, adopt, and urge the global adoption of best practices and standards associated with space systems cybersecurity. The Artemis Accords announced by the White House represent a step in the direction of improving the security of space systems globally. NIST is recognized internationally for the work that they publish. (In the development of NISTIR 8401, NIST had participation from international partners Airbus, European Space Agency and other foreign nationals.) Their publications are leveraged by other countries with less resources to devote to research in space cyber security. The Department of Commerce has a history of working internationally and has the mission for space situational awareness. Cybersecurity information is a necessary component of space situational awareness so the Department of Commerce may be an appropriate choice for international coordination on space cybersecurity.

6. In your prepared statement, you recommended that the Committee consider actions to "incentivize adoption of best practices by investing in [Research & Development] for cybersecurity technologies for space systems." During the question-and-answer portion of the hearing, you stated that the NIST National Cybersecurity Center of Excellence "has been able to help private industry adopt cybersecurity without a lot of additional costs by developing practice guides that show commercial entities that do the R&D to integrate security tools into a reference architecture to help kind of lower that entry into using [...] commercially available cybersecurity products."

a. Please expand on what types of incentives are needed to encourage commercial space to adopt cybersecurity practices.

The commercial space industry has several unique challenges to address in the adoption of cybersecurity. As stated previously commercial space is driven by the consumer and the consumer doesn't necessarily want to pay for cybersecurity. Second, space is an international domain and US commercial companies need to be competitive with international organizations that can provide the same services. Making a US company comply with regulation that is then passed on to the consumer may cause consumers to purchase services from other countries with lower or no cybersecurity in place.

Commercial space companies are very sensitive to time to market and can be slowed down by the multitude of different touch points from a regulatory perspective. Creating a single regulatory agency to oversee the licensing and regulation of commercial space will help commercial companies streamline their processes and decrees their time to market. U.S. should reform existing space regulatory structure with the agility needed to enable innovation and grant approvals on established timelines. Major delays in responding to requests for licensing or regulatory action may disincentivize prospective space companies from seeking U.S. mission authorization.

From a cybersecurity perspective the five steps of cybersecurity are identify, protect, detect, respond, and recover. Response and Recovery are reliant on cybersecurity information from the system or information on the threat being sent to the operator to then act. The Space ISAC has provided a forum for commercial space operators to share information. However, this is a voluntary organization and sharing threat information with the Space ISAC is voluntary. MITRE has worked with the Space ISAC to holds table-top exercises to show the importance of sharing information during a cyber event to prevent other organizations falling victim to the same attack. In the end cybersecurity is dependent on information and commercial space companies need to share operational cyber threat data with each other to ensure the community is more secure. Many commercial space companies do not choose to join the Space ISAC due to cost and other priorities. As part of standing up a single regulatory agency, providing funding to commercial space operators to share threat information with the Space ISAC is critical for the overall security of the sector. Without information you cannot respond and recover to a cyber incident.

b. Please provide some examples of the practices guides that these commercial entities have been using.

The practice guides I was referencing in my statement were produced by the NCCoE[4]. Currently there does not exist a practice guide for commercial space but the NCCoE has developed guides for other industries including health, energy and public safety. These guides are developed by creating a virtual IT environment representative of the industry they are focused on. Then commercial companies that have security solutions apply to participate in the development of the guide. Their participation involves the donation of their security tool to be loaded into e virtual environment which can demonstrate the functionality and protection offered by the tool. The applications are accepted on a first come first serve basis and are integrated into the representative environment. Multiple tools are integrated in the environment which is a benefit to the vendors of the tools as well as the industry because the vendors don't need to pay for a guide on how to integrate their tool with other tools. Most cybersecurity tools only address one of the 5 functions of identify, protect, detect respond and recover. It is difficult for small businesses to invest in an IT R&D project to integrated existing tools. The NCCoE can integrate the tools for a complete security solution and develop a guide on how to implement and integrate multiple tools into the businesses in the sector the guide is being developed for. The NCCoE then publishes a NIST 1800 series guide consisting of Vol A, B and C. Volume A is intended to the executive level and details the benefits of the guide. Volume B is meant for technical management so they can understand the resources required to implement the guide. Volume C consists of a step-by-step guide including screen shots that show operators how to configure multiple tools to have them work in concert to provide cybersecurity protection. As an example, the health guide has been implemented by hospitals and recommendations from the guides have also influenced manufactures of infusion pumps to adopt changes in their design based on the guide. An implementation guide like these could be developed by the NCCoE for space. A partnership between NASA, NCCoE and industry to develop practice guides like this could be

[4] Homepage | NCCoE (nist.gov)

helpful for commercial space. Commercial space operators have said that guides and best practices are needed in the industry.

c. Do small commercial space companies or new entrants face particular challenges in adopting cybersecurity best practices. If so, what are some of these challenges, and do they require additional support?

Small commercial space companies have a multitude of challenges including time to market and investor engagement. Small commercial space companies have shared with MITRE that the NASA "brand" carries weight when talking with investors. Products that have been used by NASA provide investors with the confidence that the solution being marketed by the small business company are flight worthy and will perform as expected. NASA uniquely can support these smaller companies by providing more tools and technologies that can be used by commercial space companies.

A non-technical challenge with the adoption of cybersecurity for space systems is perception. Commercial satellite companies want to ensure investors that there are minimal risks associated with the technology offering. Integrating cybersecurity tools would acknowledge there is a cybersecurity challenge.

7. What are the most important areas of research and development, including testing or demonstration activities and associated facilities, to help reduce the barriers to adoption of cybersecurity best practices in the commercial space industry? a. What, in your view, would be the major questions or challenges that are not currently being addressed and in which further investment in R&D could benefit?

The most important distinction between cybersecurity challenges as a whole and those for space systems is the need for speed. Objects in space move much faster than on the ground. Traditional cybersecurity incidents can be resolved in days but in space you need to act much more quickly. Commercial space products are not optimized for speed at the scale that space needs them to operate. Traditional cybersecurity focuses on the security of data versus maintaining positive control over a remote vehicle. Focusing R&D efforts on integration and automation of tools that can speed the response time is needed because the timely responsiveness to cyber-attacks on space systems is more acute.

As stated previously, the new paradigm for commercial space is the use of a satellite mesh that relays messages from satellite to satellite without the need to pass the message to the ground. There is a gap in the understanding of how one or more mesh networks in space will interact. In addition, there is a question on how traditional network security tools operate in a space mesh network. Model, Simulation, Emulation as well as testbeds that emulate this new space mesh network are needed.

8. During the hearing you stated that, "An attacker can be successful, regardless of the measures you put in place, making monitoring key. Monitoring and cyber situational awareness need to be built in now as part of the fabric of commercial space. You can't respond to and recover from an attack you're unaware of." a. What are some of the challenges affecting the ability of operators to closely monitor their systems and how can they be overcome?

One of the main challenges associated with monitoring for commercial space is the cost of the tools needed for monitoring and the cost of the personnel associated with implementation and maintenance of the monitoring system. Basic research is needed to that the industry understands the data elements that need to be collected from the spacecraft in order to properly analyze and determine situational awareness.

A skilled workforce to support the space and cyber domains is also limited. Investing in STEM will be critically important as the commercial space domain as it is set to increase dramatically over the next 20 years.

The speed of change within the domain is another feature of the commercial space domain. The integration of new technologies would need to be vetted before use on space vehicles. A methodology to ensure the trustworthiness of new technologies is needed to avoid an attack on the supply chain being introduced to the vehicle.

Threat information collected and used by the organization is critical but across companies is important. There is a need to share threat information across various space operators because they are all operating in the same physical space. The need to share is greater because of the need for safety of flight that is unlike anything else humans operate on earth. There is a need for neutral third party collect monitoring information across commercial space operators to ensure threats can collect scrub and anonymize the data to provide to the community. MITRE has experience creating Public, Private Partnerships such as for the FAA. The Asias model, where MITRE collected safety data from the FAA and conducted the collection anonymization of the data.

9. In your written testimony, you recommended that "consideration should be given to the designation of space systems as critical infrastructure which would provide additional emphasis to the cybersecurity and resilience of civil and commercial space systems." You also stated, in response to my question during the question-and-answer portion of the hearing, that "having space as critical infrastructure…allows there to be a focus location for commercial entities to kind of engage with the Federal Government." a. How has your work led you to this recommendation?

Answer: Overall, the designation of space systems as critical infrastructure would remedy the current situation in which there is no unified sector risk management approach for space systems. Such an approach is necessary given the importance of space systems to our national and economic security, the uniqueness of its infrastructure and technology, its singular missions, and its importance to our national economy. The need for a unified sector risk management approach has been demonstrated for other critical infrastructure sectors, without which these sectors would be vulnerable to policy and coordination gaps, overlaps, and inefficiencies.

a. The situation of the designation of space systems as a critical infrastructure sector appears to have engaged many government and industry stakeholders. My view regarding the desirability of this designation is based on several factors:

1. Sectors that are named as critical infrastructure are provided services and additional support. Information share is one of the primary benefits. In working with NIST on the cybersecurity profiles for space systems information sharing is a critical component of a robust cybersecurity strategy. CISA already shares threat information with the commercial space sector but the formalization of space as critical infrastructure will help to strengthen this effort. Other services for critical infrastructure companies include cyber security and physical security advisors that provide "free of charge" risk assessments for companies within the critical infrastructure sector which will be beneficial.
2. Every other critical infrastructure sector depends on space systems. Work done by the Space ISAC, of which we have been a member since 2019, has demonstrated the dependence of maritime, agricultural and other infrastructures on space systems. In addition, the Space ISAC has mapped dependence on space systems to the National Critical Functions.
3. Space systems have their own infrastructure, including manufacturing, launch, ground operations, and on-orbit operations, that are not covered by other critical infrastructure sectors' efforts. Some risks, including RF interference, cybersecurity risks, supply chain risks, and RF interference, are unique to space systems.
4. Space systems support unique missions not duplicated elsewhere. New commercial systems provide vital remote sensing for in support of requirements ranging from precision agriculture to US commitments to other countries and our global interests. New missions are emerging, including travel, colonization, orbital manufacturing, mining, planetary defense, and others. These missions require now or will require in future, protection of the space systems on which they depend.

5. The space systems economy will contribute directly $1 trillion by the end of the decade, and probably sooner. Unifying sector risk management for space systems would support our country's continued competitive leadership in the space domain.
6. My work in space cybersecurity is in the area of R&D and cyber security operations. My focus on the development of a federal organization dedicated to the collection and dissemination of space cyber threat data is the driving factor in the desire for space as a critical infrastructure.

b. Are there other mechanisms that could provide the same degree of focus that you describe without space being designated a critical infrastructure?

b. The current situation in which space systems are not yet designated as critical infrastructure can be sustained, but only if the various government and civil stakeholder involved treat space systems and missions as critical to our national and economic security, and if policymakers build a consistent set of sector risk management initiatives that assign responsibility and resources for the implementation of these policies. Such an approach is less desirably clearly that a critical infrastructure sector designation. In the absence of that designation, some government agencies (e.g., DHS, Space Force, and others) and commercial space sector stakeholders, convened via the Space ISAC) are undertaking as much coordination as possible.

Responses by Mr. Matthew Scholl

Questions for the Record to

Mr. Matthew Scholl

Submitted by Chairman Beyer

1. The NIST Internal Report 8270, "An Introduction to Cybersecurity for Commercial Satellite Operations," applies the NIST Cybersecurity Framework to manage cybersecurity risk to commercial satellite operations. You stated, in response to my question during the question-and-answer portion of the hearing, that, "The next steps, then, are to ensure that individual organizations really understand how to implement these processes and then potentially for us to work in an open standards body alongside industry to develop those next step things, so not necessarily NIST, internally, but now externally in a participative standards body alongside industry to grind out the next level of detail."
    a. How and when will NIST move forward on working with a participative standards body, as you describe?

NIST Response:

Currently NIST is working with the commercial space industry through several different venues, as well as during symposiums hosted by the Departments of Commerce and Homeland Security, technical workshops, and requests for private comments on cybersecurity products. Participating stakeholders include the Space Information Sharing and Analysis Center (ISAC), the Satellite Industry Association (SIA), and federal agencies who have space missions such as NASA, NOAA and the DoD. When NIST hears from industry participants that they have a need to work on space cybersecurity standards in a standards development organization for interoperability, market growth, or other needs, NIST will join them and offer NIST's work as a potential contribution. NIST also continues to work with many national and international standards bodies on the core cybersecurity items that are used in space mission areas and now bring space mission requirements into those discussions.

2. To what extent, if at all, would NIST's cybersecurity work related to space systems differ or change if space were designated a critical infrastructure sector?

NIST Response:

NIST's cybersecurity work related to space systems would not significantly differ or change if space were designated a critical infrastructure sector. If new cybersecurity requirements or regulations were to result from a critical infrastructure designation, NIST would adapt its work to ensure these were included as important considerations.

Submitted by Ms. Moore

Positioning, Navigation, and Timing (PNT) resiliency is a growing concern for stakeholders across U.S. industrial sectors and among national security experts. In addition to your written testimony that highlights the importance of reliable PNT services to our national and economic security, the National Security Council's Senior Director for Resilience and Response, Ms. Caitlin Durkovich, recently called the U.S. GPS system, which depends on reliable PNT services, "a significant single point of failure in our country," and that disruptions could lead to "cascading effects." Recent press reports of GPS jamming by Russians in Ukraine that have reinforced longstanding concerns by many U.S. stakeholders about the importance of PNT resiliency and increase the urgency to prevent catastrophic consequences disruptions or manipulations of our nation's GPS system.

1. As the U.S. considers options to harden our critical infrastructure and address PNT cybersecurity and resiliency concerns, which federal agency would you point towards as leading the government-wide implementation of resilient PNT technologies? Also, please elaborate on your views regarding the urgency of government-wide efforts to mitigate the potential impacts of a PNT disruption or manipulation and any timing for action.

NIST Response:

PNT issues span a range of technologies, deployments, and responsibilities. Space based PNT, ground antennas and receivers, different atomic clocks, and alternate positioning capabilities make a single federal agency identification a challenge. Because of this, in Space Policy Directive 7 (SPD 7), the federal government created the Space-Based Positioning Navigation and Timing National Executive Committee to lead, among other PNT priorities, the implementation of resilient PNT technologies. SPD 7 states:
"*The National Space-Based Positioning, Navigation, and Timing Executive Committee (Executive Committee) is the interagency body responsible for guiding and preserving whole-of-government interests in the provision of space-based PNT services, augmentations, and space-based alternatives. The Deputy Secretaries of the Department of Defense and the Department of Transportation, or their designated representatives, shall co-chair the Executive Committee.*"

The National Space-Based Positioning Navigation and Timing Executive Committee, hosted by the Department of Commerce Office of Space Commerce, also is responsible for identifying needed actions and publishing a five-year implementation plan to enact the provisions of SPD 7. This will establish the needed timelines and actions for government-wide efforts to mitigate the potential impacts of a PNT disruption or manipulation.

References:
https://www.gps.gov/governance/excom/
https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-7/
https://s-isac.org
https://sia.org

Responses by Mr. Brandon Bailey

Q&A for the record

Questions for the Record to
Mr. Brandon Bailey
Submitted by Chairman Beyer

1. The 2019 Aerospace Corporation paper on which you are the lead author, "Defending Spacecraft in the Cyber Domain," states that "the backbone of a cyber-resilient spacecraft should be a robust intrusion detection system."

a. What are the unique challenges for developing and implementing an intrusion detection system for space system applications and how can they be addressed?

Brandon Bailey Answer: Conceptionally intrusion detection is the backbone of Defense in Depth because in order to recover and respond to a cyber-attack, the system must know it is being attacked. As with traditional systems, we should assume a determined adversary will ultimately get in (i.e., protection has failed) therefore it will be important for the spacecraft to be able to detect the attacks and then respond and recover accordingly. Speaking specifically on intrusion detection for the spacecraft, the two largest challenges are hardware (HW) (i.e., limited capacity) and software (i.e., the logic). On the hardware side, the challenge is the size, weight, and power (SWaP) along with compute/memory limitations onboard the spacecraft. The processors currently being used have limited processing and memory capacity and adding in new functionality like intrusion detection to an already constrained environment would be difficult to achieve. For new hardware, increasing the compute and memory capacity will then have effects on the SWaP which is limited. Space system developers typically prefer to utilize hardware that has a proven track record of performing in space's harsh conditions therefore, it may be difficult to get developers to select higher performing equipment as it is developed. However, with proliferated low earth orbit (pLEO) constellations coming online there is a great opportunity to bring intrusion detection onboard the spacecraft because the HW components and architectures of the spacecraft are rapidly changing to accommodate the new mission. We should take advantage of this time of change to insert intrusion detection systems into spacecraft. The historic reluctance of space engineers to re-design should not be allowed to be a blocker of progress in spacecraft security.

The second challenge to implementation of intrusion detection is the logic piece. It has taken decades for traditional IT systems to get to where they are today with intrusion detection. These systems have evolved from the early days of anti-virus scanners that are signature based (i.e., known known fingerprint of attack) to machine learning techniques that analyzes user behaviors. Given that we have the benefit of building upon the success and failures of doing intrusion detection on traditional IT systems, putting this capability on the spacecraft should be easier. Like they do in traditional IT systems, the on-board intrusion detection must account for known-knowns as well as the unknown-unknowns. Signature based attacks are trivial, but it is the behavioral and unknown unknowns that will require the utilization of automation and machine learning on-board the spacecraft. Trades between onboard intrusion detection (in the loop) vs ground processing (out of the loop) will need to be made to balance HW resource requirements The onboard system must be able to be adaptive using machine learning along with the ability to get signature and machine learning algorithm updates in real-time from the ground or within the constellation to be able to adequately detect attacks.

2. You state in your written testimony that "space-centric cybersecurity standards and governance have been slow to materialize and are lagging behind the growth of the cyber threat." Why is that?

Brandon Bailey Answer: There are two interpretations on the question "why is that?'. From one perspective, why are standards lagging and the other is why do I feel like the threat has grown past the current standards and governance. Since this hearing was focused on commercial and civil space, the answer will be limited to that perspective. On the civil space side, there are improving standards and guidance from where the agencies were 5-10 years ago. But there is improvement needed as many of the standards and governance is focused on the traditional IT systems for the ground side which leaves the spacecraft vulnerable. The existing laws and requirements (i.e., Federal Information Security Management Act, Federal Information Processing Standards, etc.) have not been uniformly flowed down to the spacecraft. Even though a spacecraft is technically a federal information system that processes and stores federal information, it is not treated as such in practice and this has led to disjointed governance and flow down of existing regulation/requirements. If this eventually gets corrected on the civil side, translation is likely needed to the existing FISMA/FIPS and National Institute of Standards and Technology (NIST) guidance for the spacecraft. The Aerospace Corporation has performed some of this translation with TOR 2021-01333 REV A (https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft--A%20Threat%20Based%20Approach.pdf) which was provided for the record. Additional translation is likely needed as the threats and information evolves. Ultimately the civil space sector must ensure the proper security requirements are levied during their acquisition process to ensure system engineering and cybersecurity engineering occur together throughout the lifecycle. The current approach for security tends to levy compliance requirements and not engineering requirements for security. If these proper requirements are put into acquisition the existing governance structure will be enabled to hold implementers accountable for security.

On the commercial side, there is not a parallel to FISMA or FIPS therefore there are not any security requirements levied. Commercial entities are essentially free to implement security at whatever level they are comfortable with as the federal government has not levied any oversight/governance. The only policy issued was Space Policy Directive 5 which is non-binding and informational. Similarly in 2021/2022, NIST has published informational papers on cybersecurity for space systems, but these are only scratching the surface on the cyber concerns and mitigations for space systems. Where this becomes impactful to the United States is if/when the government needs to utilize these commercial assets then there is no assurance these systems are secure. The government may be consuming services without understanding the risk. This is not to imply that every commercial asset launched will require the highest level of security, but it is to say there is currently no standard a commercial asset can be certified to prove to the government that it is secure.

The secondary interpretation of this question would be "is the threat truly out pacing the standards and governance we have in place." This interpretation can be answered simply by stating we have known-known threats today in 2022 that existing standards and governance does not account for. For example, according to SPD-5 a space system must provide *"protection against unauthorized access to critical space vehicle functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats during the entire mission lifetime"*. While this is truly a best practice, there are no requirements nor governance established the ensure this is the case on the commercial side. This can be said for many of the elements in SPD-5 as well as NIST guidance. These are presented as best practices and not standards to be met or requirements that must be satisfied by law. We must establish more technical requirements to mitigate the known-known attack vectors that way we can focus on the unknown-unknows in the future.

Yet another perspective to consider is because we haven't had a high-profile cyber event on-board a spacecraft that has cost lives, considerable money, or even a war, there isn't the motivation to create proper governance or standards. The industry should be proactive rather than reactive and protect spacecraft before there is a high-profile incident.

3. How does the growing participation of international entities in space affect cybersecurity risks, and to what extent is space cybersecurity addressed on an international level?

> b. What body, in your view, is most appropriate for international coordination on space cybersecurity?
> c. What can the US do to ensure that it leads the way in the development of standards and norms for cybersecurity in space systems internationally?

Brandon Bailey Answer: Global participation is a part of current reality as space access grows. This will increase familiarity and capability with space systems. This will lower the barriers to entry to attacking space systems which increases likelihood for attacks, and therefore increases risk. As more entities, including international, put assets in space this creates opportunity for physical impacts via space debris, collision avoidance, etc. As space becomes more crowded, space situational awareness become extremely important and international collaboration and norms must be established to ensure collisions do not occur. If more assets are going into space and they do not have appropriate security in place, it presents an attack vector for adversaries to take over spacecraft or even create space-junk by disabling the operator's ability to command the spacecraft. While this may be unlikely, it must be considered as norms are being established. Using another country's spacecraft to launch attacks from (cyber or physical) must be a topic in the conversation.

As for standards and norms, the Aerospace Corporation published the following paper https://csps.aerospace.org/sites/default/files/2022-08/Dickey_CommercialNormentum_20220819.pdf for commercial norms which would/could extend into the international community. Additionally, at ASCEND 2022 the following paper was published titled "*An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action*". This paper was co-signed / co-authored by 30 different organizations which indicates the need for a standards body to address space cybersecurity. In that paper, International Electrical and Electronics Engineers Standards Association (IEEE SA) or the International Organization for Standardization were recommended to engage with for the standard development process. These standards bodies are experienced with developing and publishing international standards. As for ensuring the US leads the way, it would be recommended that they chair or lead the development of the standard within IEEE or ISO.

4. During the hearing, you noted that, "one of the things that we've done in the ISAC [Information Sharing and Analysis Center] community … is trying to translate Space Policy Directive-5 from a policy, even though it's nonbinding, to implementation details that can actually be shared in the community."

> a. Please provide more details about what this activity entails and how this effort to implement SPD-5 is proceeding.

b. What progress has the Space ISAC made in developing and disseminating cybersecurity standards to its community?
d. To what extent have government and commercial organizations engaged with the Space ISAC on developing cybersecurity standards?

Brandon Bailey Answer: From my understanding the Space ISAC, and an ISAC in general, is not a standards body and therefore they will not develop a technical standard, but they may share information related to a standard. Generically the Space ISAC has identified four driving principles for space cybersecurity which provide a solid foundation, but more detailed guidance is warranted.

- Incorporate risk management with a focus on risk assessments during the requirements phase while integrating continuous threat intelligence and threat-informed policies so security practices remain agile to emerging threats.
- Deploy risk-based, end-to-end identity and access management across space segments through the system lifecycle.
- Integrate cybersecurity leading practices and cyber capabilities for space technologies (e.g., OMB's Zero Trust strategy, CISA's Zero Trust maturity model, NIST Cybersecurity Framework and the Risk Management Framework.)
- Build for survivability and incorporate resiliency to enable systems capable of trusted recovery (e.g., build systems capable of recovering from well-known terrestrial attacks such as ransomware and known space vulnerabilities such as jamming by ensuring systems have access to timely systems patching and secure updates.)

Additionally, members of Space-ISAC are writing position papers and examining the application of cybersecurity principles like zero trust to space. Space ISAC members represent commercial industry, FFRDCs, academia, and U.S. Government and international entities; in other words, they represent everything from small academic test satellites to exquisite national security space systems. The group intends to leverage existing risk management approaches (e.g., NIST), tailor them to space, and allow developers to assess the level of risk mitigations that are aligned with their space projects.

The Space ISAC is actively engaged with their members to gather threats to space, identify recommendations, and allow the constituents to create a threat-based risk assessment identifying appropriate mitigations. Space ISAC is not a standards body and hence isn't developing standards, but they are developing best practices and other cybersecurity recommendations. Due to the vast number of variables involved in space systems (e.g., resources – money and Size Weight and Power (SWaP), mission priorities, mission lengths, orbital regime, etc.) the recommendations will not be "one size fits all" but will allow tailoring. Tailoring is a must for space cybersecurity. The cyber threat environment and cyber risk for low earth orbit to cis-lunar to deep space vary which will require different levels of cybersecurity. The Space ISAC continually publishes resources on their website: https://s-isac.org/resources/. Additionally, in August 2022, the Space ISAC established the Space Threat Resource & Intelligence Knowledge Exchange (STRIKE) Task Force to better share more tactical information related to cybersecurity for space systems. STRIKE will also review potential best practices for endorsement by the ISAC that can be shared via the communication channels within the ISAC community.

Stakeholders are eager to address cybersecurity risks; recent events have further demonstrated cyber risk is a key threat to mission assurance. As Space ISAC is a relatively young and developing organization the government and commercial members are enthusiastic but actionable results will require some impartial leadership to obtain faster and more robust recommendations. It is generally accepted that detailed government technical recommendations are often outdated before they can go through legal and regulatory processes. Therefore, it is recommended that industry helps define the cybersecurity recommendations in conjunction with government through Space ISAC through a joint working group.

5. Following the cyberattacks launched in February 2022 on commercial satellite communication networks in Ukraine, attributed to Russian state-sponsored malicious cyber actors, at least three federal agencies were involved in issuing space cyber alerts. The Cybersecurity and Infrastructure Security Agency and the FBI issued a cyber alert for satellite communication providers. In addition, the National Security Agency issued a cybersecurity recommendation on protecting very small aperture terminal networks. Is there a single agency that has responsibility for cybersecurity for space? If not, should there be?

Brandon Bailey Answer: No there is not a single agency, nor should there be a single agency that is responsible for cybersecurity for space. Multiple agencies have multiple areas of influence and information access therefore, in the federal government there isn't a single entity responsible for cybersecurity for space. All of these agencies should continue to work together and ensure that the government is not issuing conflicting guidance to the community. Based on the Ukraine incident, it appears these agencies did work together as the majority of the information was uniform. In parallel to the government issuing information, commercial entities were also putting information out (i.e., ViaSat, Sentinel One, SpaceX). This presents an interesting scenario for the space community when dealing with cyber that impacts both commercial and government. Information that may be sensitive from a government perspective, may be freely being shared by commercial entities. The government must understand this information distribution pathway and deconflict if/when conflicts arise.

However, as stated in my written and verbal testimony if "space technology" is identified as a critical infrastructure sector then a sector risk management agency must be established. This does not mean that one agency should necessarily rule them all, but it does mean that the section risk management agency (SRMA) should be the coordination body among all the other applicable agencies to ensure a uniform information is being distributed. Someone should be aggregating and ensuring information from DHS, NSA, FBI along with commercially provided data does not conflict and provides value to the community.

6. In your written testimony, you stated that there is a "likely need to create a dedicated space technology [critical infrastructure] sector," and that designating space as critical infrastructure "would stimulate policy and stakeholder attention and resources needed to secure the space systems that support the [National Critical Functions]…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…[and] 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."

a. Are there other mechanisms that could provide the same degree of focus that you describe without space being designated a critical infrastructure?

b. Are there examples from other industries where the designation as critical infrastructure has led to increased resources to address cybersecurity challenges and has resulted in reduced cybersecurity incidents?
c. To what extent would a critical infrastructure designation potentially affect the costs to develop space systems and the requirements levied on the commercial space industry?

Brandon Bailey Answer:

- a: Within the current federal governance structure, I do not believe there is an alternative method. Presidential Policy Directive 21 was created to protect our nation's critical infrastructure which space technology is essential to all 55 national critical functions. There is always an opportunity to create something entirely new and unique, but the federal government already has the infrastructure, procedure, understanding outlined by PPD-21 therefore this appears to be the only mechanism currently available to unify and set the United States up for success on securing the space environment.
- b: While it is hard for me to measure "reduced cybersecurity incidents" as this is a false negative from a metrics perspective, I can assert that cybersecurity improvements have been seen within the critical infrastructure sectors in the last 10 years. Many of these sectors have had dedicated efforts to address the cybersecurity issues within each sector. For example, the Energy Sector developed a plan in 2015 https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf where they establish methods to measuring progress against the stated goals in the plan. See Table 6-1 Energy Sector Activities Mapped to Joint National Priorities of that plan. I would have to defer to that sector risk management agency on the efficacy of their approach but as an outsider to the sector, cybersecurity has improved.
- c: Cybersecurity is not implemented for free. Implementing anything will have cost. The cost of doing nothing and having catastrophic space system failure is almost certainly more costly than performing focused cybersecurity protections. The key will be what protections are levied from a regulatory perspective. This is where the SRMA and their levied regulations/requirements are extremely important and must be implemented correctly by knowledgeable subject matter experts using threat-informed risk-based engineering. As stated in the written testimony, "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."

7. During the hearing, you stated, "on the commercialization of space that we're … starting to see a little more commoditized standard technology that's being used, and open source software that's being used that we haven't seen in the past. So I think the supply chain aspect is going to be of increasing importance with the commercialization of space because now you're seeing entities run like real-time Linux on spacecraft where before you would never see that."

a. Are you aware of the extent to which commercial IT systems now being used on spacecraft are monitored for supply chains cybersecurity intrusions? If so, please discuss this monitoring and explain how it may need to be adjusted or modified to meet the needs of space systems.
b. To what extent do Federal agencies collaborate and coordinate their cybersecurity-related guidance and/or requirements for government contracts or agreements for commercial space systems or services?
c. To your knowledge, are there standard Federal guidelines and/or requirements regarding cybersecurity for government contracts or other agreements for the acquisition of commercial space systems or services? If so, what are they?

Brandon Bailey Answer:

- a: To clarify my position, my statement about commoditized technology means that there is more opportunity and return on investment for adversaries to attack the supply chain to impact space systems. In the legacy environment for space systems, everything was built as mostly one-off implementations (i.e., the boutique model) where attacking that supply chain may impact a single system. With constellation-based proliferated low earth orbit (pLEO) in conjunction commoditized technology, supply chain attacks are much more attractive. Due to this increased risk where an adversary can attack the supply chain and impact multiple spacecraft or space systems, much more focus should be applied for protection. This isn't unique to the space enterprise, and many of the best practices from the traditional information technology sector apply to space. However, the difference is that traditionally the space enterprise has rather closed supply chains therefore it may not have been a concern in the past.
- b: The federal government has been issuing recommendations on supply chain protection in general via NIST publications. These are non-binding guidelines but are good information, nonetheless. The federal government and NIST should continue to put out information, but there needs to be focus on making these guidelines or a sub-set of them binding and requirements vice nice to haves.
- c: On the civil space side there are guidelines issued through FISMA and FIPS which point to the NIST Risk Management Framework. Within RMF there are numerous supply chain controls that are levied, in fact in revision 5 there is an entire control family dedicated to supply chain (i.e., the SR family. - https://csf.tools/reference/nist-sp-800-53/r5/sr/)

8. During the hearing, you noted that, "If done properly, having a space domain-knowledgeable governance structure can help establish better cybersecurity standards and information sharing across the community." What are the attributes of a governance structure that could affect these changes?

Brandon Bailey Answer: My position on having space domain-knowledgeable entities involved was meant to convey that space is a unique environment and translation is often needed from general guidelines and best practices to how it applies to the space system. The intent was to communicate the necessity that domain aware entities must be involved to establish the right standards. For example, saying “follow NIST Risk Management Framework” as a solution to space cyber standards will not suffice. More detailed, domain specific information is required. This is the reason NIST published NISTIR 8270 as it was to begin the conversation and fostering better translation, but the community and government must extend past high level guidelines and focus on implementation guidance and detailed standards to address the threat in an effective manner.

The attributes necessary would be

- Understands world-wide ground communication networks that support space communications
- Understands the constraints of operating in harsh outer space conditions along with low size, weight, power, and compute/memory capacity
- Awareness of how to secure embedded real time operating systems and translating/applying federal regulation to these system
- Experience with working with space-based industry partners and Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs) that focus on space systems
- Experience with working within the federal governance structure and understands the roles and responsibilities of each space agency (i.e., NOAA, NASA, Space Force, Air Force, etc.)
- Has full understanding of existing regulation FISMA, FIPS, NIST, and awareness of Committee on National Security Systems 1253 along with the space overlay