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.