U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Opening Statement

Chairman Don Beyer (D-VA)
of the Subcommittee on Space and Aeronautics

Space and Aeronautics Subcommittee Hearing
Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial Space Systems

July 28, 2022

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.