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

Opening Statement

Chairwoman Eddie Bernice Johnson (D-TX)

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

July 28, 2022

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.