



COMMITTEE ON SCIENCE SPACE & TECHNOLOGY

REPUBLICANS

Opening Statement of Ranking Member Brian Babin

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

July 28, 2022

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.