MARCH 28, 2023

Readout of Space Systems Cybersecurity Executive Forum Hosted by the Office of the National Cyber Director and the National Space Council

▸ BRIEFING ROOM ▸ STATEMENTS AND RELEASES

This afternoon, the Office of the National Cyber Director (ONCD) and the National Space Council convened government and private-sector leaders for a forum focused on bolstering cybersecurity in the space systems ecosystem. This forum took place as part of a larger series of executive-level meetings hosted by ONCD targeting various sectors, including most recently an electric vehicles and electric vehicle supply equipment-focused event in October 2022. The Space Forum was designed to facilitate robust discussion on this topic at the executive level and drive action to motivate critical cybersecurity investments across the space systems ecosystem.

Kemba Walden, Acting National Cyber Director, and Chirag Parikh, Deputy Assistant to the President and National Space Council Executive Secretary, hosted Don Graves, Deputy Secretary, Department of Commerce; Bill Nelson, Administrator, National Aeronautics and Space Administration (NASA); Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber & Emerging Technology, National Security Council; Cara Abercrombie, Deputy Assistant to the President and Coordinator for Defense Policy and Arms Control, National Security Council; General David Thompson, Vice Chief of Space Operations, United States Space Force; and other senior government officials and senior executives representing diverse elements of the U.S. space industry for a cyber threat briefing and a roundtable discussion on cybersecurity. U.S. Government officials emphasized the need to partner closely with the private sector to ensure the resiliency of the U.S. space ecosystem against cyber threats.

Industry participants — including from the satellite communications, launch, imagery, cloud and data, cross-functional defense systems and services, and venture capital elements of the space industry — shared their organizations' views on current space system cybersecurity practices including strategies for executives to measure cyber risk, addressing supply chain challenges, deploying quantum resistant cryptographic algorithms, and the need to better secure open source libraries. Attendees discussed recommendations to build on existing policy, including Space Policy Directive-5, "Cybersecurity Principles for Space Systems," to mitigate cybersecurity vulnerabilities and address cyber threats. Government officials noted the need for tangible, comprehensive guidance for government and commercial space system developers and operators to measurably improve the cybersecurity of their space systems in the current threat environment. Government officials also shared that the Biden-Harris Administration's new National Cybersecurity Strategy outlines an affirmative vision for building digital and space systems ecosystem that is more inherently defensible, resilient, and aligned with U.S. values, which applies equally to the space systems ecosystem. All participants emphasized the importance and urgency of executive-level attention on shoring up the resilience of U.S. space systems through increased investments in cybersecurity.

Public and private sector space actors — including stakeholders representing the diversity of the space ecosystem — must work together to proactively address cybersecurity challenges. Toward this objective, the following commitments were made:

- In the coming months, the Office of the National Cyber Director will convene workshops in regional hubs for U.S. space industry innovation to understand (1) industry perspectives on current policy for cybersecurity of space systems, including Space Policy Directive-5, and (2) gaps requiring more specific guidance and tangible next steps that the White House could build upon;
- The Department of Commerce will hold a Space Cybersecurity Symposium in Washington, D.C., with participation from a broad range of public and private space and cybersecurity stakeholders; and,
- The National Institute of Standards and Technology (NIST) will finalize its report, "Introduction to Cybersecurity for Commercial Satellite Operations," this fiscal year, providing a method for applying the NIST Cybersecurity Framework to commercial space activities and a set of cybersecurity outcomes, requirements, and suggested controls.

###