Space Policy Directive-5

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF HOMELAND SECURITY
THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
THE DIRECTOR OF THE NATIONAL RECONNAISSANCE OFFICE
THE ADMINISTRATOR OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
THE DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
THE CHAIRMAN OF THE FEDERAL COMMUNICATIONS COMMISSION

SUBJECT: Cybersecurity Principles for Space Systems

Section 1. Background. The United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications. Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure.

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.

The National Security Strategy of December 2017 states that "[t]he United States must maintain our leadership and freedom of action in space." As the space domain is contested, it is necessary for developers, manufacturers, owners, and operators of space systems to design, build, operate, and manage them so that they are resilient to cyber incidents and radio-frequency spectrum interference.

Space Policy Directive-3 (SPD-3) of June 18, 2018 (National Space Traffic Management Policy), states that "[s]atellite and constellation owners should participate in a pre-launch certification process" that should consider a number of factors, including encryption of satellite command and control links and data protection measures for ground site operations.

The National Cyber Strategy of September 2018 states that my Administration will enhance efforts to protect our space assets and supporting infrastructure from evolving cyber threats, and will work with industry and international partners to strengthen the cyber resilience of existing and future space systems.

Sec. 2. Definitions. For the purposes of this memorandum, the following definitions shall apply:

(a) "Space System" means a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service. A space system typically has three segments: a ground control network, a space vehicle, and a user or mission network. These systems include Government national security space systems, Government civil space systems, and private space systems.

(b) "Space Vehicle" means the portion of a space system that operates in space. Examples include satellites, space stations, launch vehicles, launch vehicle upper stage components, and spacecraft.

(c) "Positive Control" means the assurance that a space vehicle will only execute commands transmitted by an authorized source and that those commands are executed in the proper order and at the intended time.

(d) "Critical space vehicle functions (critical functions)" means the functions of the vehicle that the operator must maintain to ensure intended operations, positive control, and retention of custody. The failure or compromise of critical space vehicle functions could result in the space vehicle not responding to authorized commands, loss of critical capability, or responding to unauthorized commands.

Sec. 3. Policy. Cybersecurity principles and practices that apply to terrestrial systems also apply to space systems. Certain principles and practices, however, are particularly important to space systems. For example, it is critical that cybersecurity measures, including the ability to perform updates and respond to incidents remotely, are integrated into the design of the space vehicle before launch, as most space vehicles in orbit cannot currently be physically accessed. For this reason, integrating cybersecurity into all phases of development and ensuring full life-cycle cybersecurity are critical for space systems. Effective cybersecurity practices arise out of cultures of prevention, active defense, risk management, and sharing best practices.

The United States must manage risks to the growth and prosperity of our commercial space economy. To do so and to strengthen national resilience, it is the policy of the United States that executive departments and agencies (agencies) will foster practices within Government space operations and across the commercial space industry that protect space assets

and their supporting infrastructure from cyber threats and ensure continuity of operations.

The cybersecurity principles for space systems set forth in section 4 of this memorandum are established to guide and serve as the foundation for the United States Government approach to the cyber protection of space systems. Agencies are directed to work with the commercial space industry and other non-government space operators, consistent with these principles and with applicable law, to further define best practices, establish cybersecurity-informed norms, and promote improved cybersecurity behaviors throughout the Nation's industrial base for space systems.

Sec. 4. Principles. (a) Space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering. Space systems should be developed to continuously monitor, anticipate, and adapt to mitigate evolving malicious cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations. Space system configurations should be resourced and actively managed to achieve and maintain an effective and resilient cyber survivability posture throughout the space system lifecycle.

(b) Space system owners and operators should develop and implement cybersecurity plans for their space systems that incorporate capabilities to ensure operators or automated control center systems can retain or recover positive control of space vehicles. These plans should also ensure the ability to verify the integrity, confidentiality, and availability of critical functions and the missions, services, and data they enable and provide. At a minimum, space system owners and operators should consider, based on risk assessment and tolerance, incorporating in their plans:

(i) Protection against unauthorized access to critical space vehicle functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats during the entire mission lifetime;

(ii) Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems;

(iii) Protection against communications jamming and spoofing, such as signal strength monitoring programs, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures designed to provide security against existing and anticipated threats during the entire mission lifetime;

(iv) Protection of ground systems, operational technology, and information processing systems through the adoption of deliberate cybersecurity best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems, including from insider threats. Such practices include logical or physical segregation; regular patching; physical security; restrictions on the utilization of portable media; the use of antivirus software; and promoting staff awareness and training inclusive of insider threat mitigation precautions;

(v) Adoption of appropriate cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements such as information systems, antennas, terminals, receivers, routers, associated local and wide area networks, and power supplies; and

(vi) Management of supply chain risks that affect cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.

(c) Implementation of these principles, through rules, regulations, and guidance, should enhance space system cybersecurity, including through the consideration and adoption, where appropriate, of cybersecurity best practices and norms of behavior.

(d) Space system owners and operators should collaborate to promote the development of best practices, to the extent permitted by applicable law. They should also share threat, warning, and incident information within the space industry, using venues such as Information Sharing and Analysis Centers to the greatest extent possible, consistent with applicable law.

(e) Security measures should be designed to be effective while permitting space system owners and operators to manage appropriate risk tolerances and minimize undue burden, consistent with specific mission requirements, United States national security and national critical functions, space vehicle size, mission duration, maneuverability, and any applicable orbital regimes.

Sec. 5. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(d) The Secretary of Commerce is authorized and directed to publish this memorandum in the *Federal Register*.