THE WHITE HOUSE

President Donald J. Trump is Establishing America's First Comprehensive Cybersecurity Policy for Space Systems

"Every day, America's adversaries are testing our cyber defenses. They attempt to gain access to our critical infrastructure, exploit our great companies, and undermine our entire way of life. And we can't let that happen."
— President Donald J. Trump

PROTECTING AMERICAN SPACE SYSTEMS FROM CYBER THREATS: President Donald J. Trump's Space Policy Directive – 5 is the Nation's first comprehensive cybersecurity policy for space systems. SPD-5 establishes key cybersecurity principles to guide and serve as the foundation for America's approach to the cyber protection of space systems.

- Space systems enable key functions such as global communications; positioning, navigation and timing; scientific observation; exploration; weather monitoring; and multiple vital national defense applications. These systems, networks, and channels can be vulnerable to malicious activities that can deny, degrade, or disrupt space operations, or even destroy a satellite. 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 Policy Directive-5 fosters practices within U.S. Government and commercial space operations that protect space assets and their supporting infrastructure from cyber threats.

- SPD-5 furthers the policies and objectives of the National Security Strategy, the National Cyber Strategy, and SPD-3 (National Space Traffic Management Policy) to ensure the Nation maintains its leadership and freedom of action in space. It provides guidance on the protection of space assets and supporting infrastructure from evolving cyber threats and mitigates the potential for the creation of harmful space debris resulting from malicious cyber activities.

- SPD-5 recognizes that cybersecurity principles and practices that apply to terrestrial systems also apply to space systems; encourages integrating cybersecurity into all phases of space systems development; and stresses that effective cybersecurity practices stem from cultures of prevention, active defense, risk management, and the sharing of best practices.

- SPD-5 directs U.S. Government agencies to work with commercial companies consistent with the principles in the SPD to further define best practices, establish cybersecurity informed norms, and promote improved cybersecurity behaviors throughout the Nation's industrial base for space systems.

- SPD-5 establishes the following cybersecurity principles for space systems:

- Space systems and their supporting infrastructure including software, should be developed and operated using risk-based, cybersecurity-informed engineering;

- Space systems operators should develop or integrate cybersecurity plans for space systems that include capabilities to: protect against unauthorized access; reduce vulnerabilities of command, control and telemetry systems; protect against communications jamming and spoofing; protect ground systems from cyber threats; promote adoption of appropriate cybersecurity hygiene practices; and, manage supply chain risks;

- Space system cybersecurity requirements and regulations should leverage widely-adopted best practices and norms of behavior;

- Space system owners and operators should collaborate to promote the development of best practices and mitigations; and

- Space systems operators should make appropriate risk trades when implementing cybersecurity requirements specific to their system.