wiley

ALERT

White House Issues Space Policy Directive on Cybersecurity

September 8, 2020

On September 4, 2020, the Trump Administration issued a policy directive on "Cybersecurity Principles for Space Systems" (SPD-5). This is the fifth in a series of directives from the White House on space policy and the first to focus primarily on cybersecurity. SPD-5 applies to "space systems," including ground systems, sensor networks, and space vehicles providing space-based services. SPD-5 therefore has broad implications for satellite manufacturers, owners, operators, and their supporting industries.

SPD-5 clarifies that "[c]ybersecurity principles and practices that apply to terrestrial systems also apply to space systems," but that certain principles and practices are "particularly important to space systems." To that end, SPD-5 adopts five cybersecurity principles to guide the government's approach to space system cybersecurity:

- Space systems, including software, should be developed and operated using "risk-based, cybersecurity-informed engineering" that enable systems to "continuously monitor, anticipate, and adapt to mitigate evolving malicious cyber activities." (Sec. 4(a)).
- Owners and operators of space systems should develop cybersecurity plans to retain or, if necessary, recover positive control of space vehicles. At a minimum, plans should consider, based on risk assessment and tolerance, incorporating:
    - Protections against unauthorized access to critical space vehicle functions, including protection of command, control, and telemetry links using "validated authentication or encryption measures;" (Sec. 4(b)(i))

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jennifer D. Hindin
Partner
202.719.4975
jhindin@wiley.law

Madeleine M. Lottenbach
Partner
202.719.4193
mlottenbach@wiley.law

Practice Areas

Space and Satellite

Telecom, Media & Technology

  - Physical protections to minimize space vehicle command, control, and telemetry receiver system vulnerabilities; (Sec. 4(b)(ii))
  - Protections against jamming or spoofing of communications, for example, through "signal strength monitoring programs, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures;" (Sec. 4(b)(iii))
  - Protections for "ground systems, operational technology, and information processing systems," using best practices identified in the NIST Cybersecurity Framework; (Sec. 4(b)(iv)
  - For network elements and information systems, adoption of cyber hygiene best practices, physical security for automated information systems, and intrusion detection methodologies; (Sec. 4(b)(v)) and
  - Supply chain risk management, for example, through source verification and product tracking. (Sec. 4(b)(vi))
- Regulators should implement these principles through the adoption of rules and regulatory guidance, "including through the consideration and adoption, where appropriate, of cybersecurity best practices and norms of behavior." (Sec. 4(c))
- Space system owners and operators should collaborate to promote the development of best practices, as well as share "threat, warning, and incident information within the space industry" using Information Sharing and Analysis Centers. (Sec. 4(d))
- Design security measures should be effective but flexible, permitting owners and operators to manage "appropriate risk tolerances and minimize undue burden, consistent with specific mission requirements." (Sec. 4(e))

Cybersecurity has been an increased focus of the federal government and regulators in recent years, and the space industry is no exception. Although SPD-5 does not direct a specific agency to implement these principles, it instructs executive agencies generally to build upon—through "rules, regulations, and guidance,"—other space policies put forward by the Administration. For example, Space Policy Directive-3 on "National Space Traffic Management" calls for a pre-launch certification process that considers, among other things, whether the proposed constellation includes "encryption of satellite command and control links and data protection measures for ground site operations."

Executive agencies have already begun incorporating cybersecurity principles into their respective regulations consistent with previous space directives. For instance, the Federal Communications Commission clarified this year that its existing rule on transmitting station control, Section 25.271, requires space station operators to secure satellite commands against unauthorized access and use.

The space and space-supporting industries should therefore continue to monitor cybersecurity developments and prepare to engage with regulators as they examine how best to enhance cybersecurity in the space sector. As SPD-5 suggests, future rules or guidance may not be limited to space vehicles, but also include ground components and networks supporting space-based services. Future regulations or guidance could have far-reaching effects.