CLIENT ALERT

New National Cyber Strategy Outlines President's Cyber Agenda

Oct.05.2018

On September 21st, the president issued the National Cyber Strategy setting forth the administration's cybersecurity initiatives and regulatory and legislative agenda. It follows the May release of the Department of Homeland Security Cybersecurity Strategy and is part of a continued push by the federal government to ensure cybersecurity remains a policy priority.

The strategy calls for a dual emphasis on technical advancements and greater administrative efficiency, and it contains four key "pillars":

- Managing cybersecurity risks to increase the security and resilience of the federal government's information and information systems and protect domestic networks, system, functions, and data.
- Preserving U.S. influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency.
- Identifying and thwarting behavior in cyberspace that is destabilizing and contrary to national interests by deterring and, if necessary, punishing bad actors.
- Preserving the long-term interoperability, security, and reliability of the Internet in support of U.S. interests.

U.S. Government Priorities

To implement its goals, the strategy emphasizes several practical steps for the federal government. First, the administration intends to pursue the centralization of federal civilian cybersecurity operations implemented by DHS, while Defense and Intelligence Community authorities will remain independent. The strategy details the administration's plan to streamline federal civilian cybersecurity, investigation, and incident response by consolidating cyber resources within DHS, and previews that "new policies and architectures" are likely forthcoming for both federal agencies and the private sector. Increased cooperation by federal authorities will be emphasized both internally among the various agencies and externally with private industry. In particular, the administration intends to "ensure DHS has appropriate access to agency information systems for cybersecurity purposes" and authorize the agency to "take and direct action to safeguard systems from the spectrum of risks." The strategy also indicates that incident response will be specifically targeted for improvement as a means of combatting cybercrime and decreasing cybersecurity risk.

Additionally, the strategy contains the administration's first legislative goal in the cyber arena: to "work with Congress to update electronic surveillance and computer crime statutes." This may indicate an intention to pursue legislative action to update major federal authorities such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act – statutes increasingly referred to as outdated in the modern technological environment.

Throughout, the strategy emphasizes the administration's focus on deterrence as a tool for dealing with cyber adversaries. The administration makes plain its willingness to deter "activity that is contrary to responsible behavior in cyber-space" through both

"cyber and non-cyber means." The administration specifically references targeting both malicious actors and their sponsors via "all instruments of national power."

International Cooperation

The administration emphasizes its intention to work with international partners in order to combat adversaries and maintain competitiveness in the cybersecurity market. Specifically, the administration intends to launch an international Cyber Deterrence Initiative as part of its broader enforcement posture. Bringing together "like-minded states," the initiative will "develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior." The initiative will also focus on sharing automated and actionable cybersecurity information, particularly in the realm of threat attribution, to enable quicker and more effective international responses to cyber threats.

Working with the Private Sector

In addition to strengthening cybercrime reporting and legislation, a significant portion of the strategy focuses on how the federal government will work with the private sector to advance its cybersecurity agenda. A major component of that initiative is the minimization of supply chain risk and enhancement of government contractor cybersecurity, reflecting a persistent theme over the past year that cybersecurity is becoming a key factor in the procurement process. Significant priorities affecting contractors include:

- Improving supply chain risk management by sharing supply chain threats between agencies.
- Creating a supply chain risk assessment shared service that would exchange findings between agencies.
- Developing streamlined authorities to exclude vendors determined to have unsafe cybersecurity practices.
- Reviewing contractor risk management practices and adequately testing, detecting, and responding to incidents on contractor systems.
- Drafting future contracts with federal departments and agencies to authorize risk management and cybersecurity assessments.

The administration's thorough recitation of cybersecurity priorities in the strategy demonstrates its increased emphasis on cybersecurity. It also signals a commitment to advance cybersecurity policy through new legislation, regulation, enforcement strategies, and an increased use of federal buying power to drive private sector best practices. Businesses that contract directly with the government and those in the government supply chain should be prepared for increased focus on cybersecurity issues during both the initial procurement and audit parts of the process.

The strategy will likely foreshadow similarly themed regulations and enforcement practices to come. In the meantime, the administration has tasked the National Security Council with implementing this policy through coordination with federal agencies and the Office of Management and Budget.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1 202.624.2545
Email: mgruden@crowell.com