Van Ness Feldman LLP
vnf.com

Trump Administration Moves to Address Cybersecurity Concerns, Congress Funds Cyber Programs

SEPTEMBER 26, 2018

Tracy Nagelbush *and* *Michael Weiner*

On September 21, 2018, the Trump Administration released a National Cybersecurity Strategy ("Strategy"), to define its national cybersecurity policy and implement efforts to streamline responsibilities for mitigation and responses to cybersecurity events across federal agencies. This Strategy also addresses working with the private sector to protect assets, train the workforce and mitigate any future cyber-attacks.

The National Cybersecurity Strategy, a statement of Administration policy rather than a Presidential directive, builds on prior efforts by the Obama Administration to develop a comprehensive and coherent nationwide strategy to promote cybersecurity across multiple levels of government and among myriad industries. While other agencies—notably the Departments of Defense and Homeland Security—have issued more narrowly-tailored plans and policies, this is the first major cybersecurity document to apply to the entire federal government. The Strategy provides an important glimpse into the current Administration's plan to address the ever-increasing cyber threats to national security imposed by malicious nation-state, non-state, and independent actors.

Specifically, the Strategy identifies four major areas of focus that may be of interest to stakeholders:

- **Supply Chain Risk Management.** Through this Strategy, the Administration directs federal agencies to integrate supply chain risk management practices into agency procurement and traditional risk management processes, including the creation of a supply chain risk assessment shared service to reduce duplicative supply chain activities across federal agencies. The Strategy also mandates federal investment in more secure supply chain technologies. There are several bills pending before the Congress that would mandate requirements for supply chain risk management for federal agencies into law, including S. 3085, the "Federal Acquisition Supply Chain Security Act of 2018". This bill was reported favorably by the Senate Homeland Security and Governmental Affairs Committee on September 26th. (More information on S. 3085 is available here.)

- **Strengthening Information Sharing Efforts.** The Strategy commits to strengthen information sharing efforts in order to protect critical infrastructure assets and allow information and communications technology (ICT) providers to respond to malicious cyber activity in a more timely and effective manner. These actions include sharing threat and vulnerability information with cleared ICT operators, declassifying information as much as possible, and promoting an adaptable, sustainable and secure technology supply chain.

- **Building a Robust Cybersecurity Workforce.** The Strategy outlines actions the Administration will take to recruit and maintain a highly skilled cybersecurity workforce through the expansion of Federal recruitment and training efforts, while also re-skilling employees into cybersecurity careers. It also will explore the capability of maintaining distributed cybersecurity personnel at the Department of Homeland Security that can be deployed across Federal agencies. There are several bills pending before the Congress that would create an employee rotation for government workers focused on cybersecurity. Among them, S. 3437 the "Federal Rotational Cyber Workforce Program Act of 2018" was reported favorably by the Senate Homeland Security and Governmental Affairs Committee on September 26th. (More information on S. 3437 is available here.)

- **Deterrence and Offensive Capabilities.** The Strategy authorizes federal agencies to conduct counter-offensive or "hack back" operations against malicious actors. This continues the Administration's departure from policies of previous Administrations, including its August decision to rescind Presidential Policy Directive 20, which governed the federal agency approval process for offensive cyber operations.

Recent Congressional Actions on Cybersecurity

In addition to the initiatives specifically outlined above, both chambers of Congress have taken additional steps to address cybersecurity across critical infrastructure sectors. Importantly, Congress agreed to provide funding and direction for the newly-created Office of Cybersecurity, Energy Security, and Emergency Response (CESER) within the Department of Energy. The recently enacted FY 2019 Energy and Water, Development and Related Agencies Appropriations bill, which was part of a broader funding package signed into law by the President on September 21, 2018, included $120 million for the CESER office and specific direction that funding be applied to research and development focusing on supply chain risks. This research may tackle how IT systems, software, and networks pose legitimate cyber risks to the broader infrastructure they serve, including through malware and unknown software vulnerabilities. The summary and text of the Appropriations bill is available here.

Additionally, this week, the House Energy and Commerce Subcommittee on Energy will hear testimony from Karen Evans, Assistant Secretary for CESER, as a part of its "DOE Modernization" hearing series. Committee members are likely to question Ms. Evans on CESER's role in the implementation of the Strategy, as well as issues including securing energy infrastructure from cybersecurity threats, public-private partnerships, and electricity grid resilience. Additional information on this hearing is available here.

Outlook

The Strategy is the first step for the Administration to define broader cybersecurity threats and begin to develop a cohesive plan to combat cyber-attacks. The document itself does not contain many specific imminent actions that the Administration will take and questions remain over who within the Trump Administration is personally responsible for coordinating these and other cybersecurity efforts.

The Strategy does, however, identify areas in which the Administration will seek to work with Congress on legislative solutions to promote these goals. For example, the document specifically references efforts to work with Congress to "update electronic surveillance and computer crime statutes" to better enable law enforcement to deter criminal activity. Further, the Administration indicates it will work with the Congress to promote education and training opportunities to develop a robust cybersecurity workforce. Congress has been innately focused on cyber workforce issues already, with a slate of existing bills introduced by members of both parties to strengthen education and training programs in this area as noted above.

With midterm elections looming in 41 days, both Democrats and Republicans in Congress are preparing their legislative agendas for the 116th Congress set to convene in January. Democrats and Republicans alike have indicated that cybersecurity will be at the top of the legislative agenda. Whether it is through action on election security, autonomous vehicles, electric utility stabilization policies, or other critical infrastructure areas, cybersecurity will continue be a major topic of discussion through 2019.

For more information

The Van Ness Feldman cybersecurity team will issue further alerts analyzing the effect of the midterm election results on the rapidly-evolving cybersecurity legal and policy landscape in the 116th Congress. If you have questions about the National Cybersecurity Strategy or any other recent cyber developments, please contact Gwen Keyes Fleming, R. Scott Nuzum, Tracy Nagelbush, Darshana Singh, Mike Weiner, or any member of the firm's Cybersecurity practice at (202) 298-1800 in Washington, D.C. or in Seattle at (206) 623-9372.

Follow us on Twitter @VanNessFeldman

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.