Published on *The National Law Review* https://natlawreview.com

It’s Here – The New National Cybersecurity Strategy

Article By:

Kurt R. Erskine

Romaine C. Marshall

Today, after months of rumors regarding its release and contents, the White House issued its National Cybersecurity Strategy “to secure the full benefits of a safe and secure digital ecosystem.”[1] The full strategy is 39 pages and divided into five pillars, the first of which is titled “Defend Critical Infrastructure.”[2]

The Strategy will take weeks and months to unpack, and perhaps years for the public and private sectors to agree on what is necessary and relevant for their industries and programs. For example, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted a year ago, is not expected to be finalized and enforced until next year.

Nevertheless, the Strategy is bold and concise as to why a coordinated strategy must stem the rising tide of cyberattacks. It points to emerging trends and malicious actors, notably calling out the “governments of China, Russia, Iran, and North Korea” as the culprits threatening national security, and criminal syndicates threatening economic prosperity.

As to Pillar One, the Strategy focuses on the *availability* of sixteen sectors (shown below) whose assets, systems, and networks, whether physical or virtual, are considered so critical that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Determined to be “a model for critical infrastructure,” Pillar One of the Strategy is divided into five strategic objectives that prominently feature the federal government’s own systems:

1. Establish Cybersecurity Requirements to Support National Security and Public Safety
2. Scale Public-Private Collaboration
3. Integrate Federal Cybersecurity Centers
4. Update Federal Incident Response Plans and Processes
5. Modernize Federal Defenses

As shown by the *Executive Order on Improving the Nation's Cybersecurity* released in May 2021, a patchwork of laws, regulations and industry standards have emerged within certain private sectors. We lightly covered those impacting the energy, water and wastewater, transportation systems, government facilities, emergency services, and water and wastewater sectors.[3]

Naysayers may criticize the Strategy for being vague and ambiguous. On the other hand, those entities paying close attention to key governance structures – e.g., incident response plans, risk assessments and written information security programs – can use the Strategy to further fulfill related obligations for executive oversight and vendor management.

FOOTNOTES

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[2] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] https://www.polsinelli.com/romaine-c-marshall/publications/looting-of-local-governments-leads-to-cybersecurity-standards-for-the-water-and-wastewater-sector, https://www.polsinelli.com/romaine-c-marshall/publications/for-ot-cybersecurity-extra-time-is-running-out, and https://www.polsinelli.com/romaine-c-marshall/publications/national-security-focus-on-cybersecurity-for-critical-infrastructure-sharpens.

National Law Review, Volume XIII, Number 61