July 19, 2023

# White House Signals Additional Private Sector Cyber Obligations as Part of National Cybersecurity Strategy Implementation Plan

On July 13, the White House released its National Cybersecurity Strategy Implementation Plan (NCSIP), laying out its strategic plans for pursuing the goals identified in the updated National Cybersecurity Strategy released on March 2[1] and doubling down on the Administration's call for "fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace to ensur[e] that the biggest, most capable, and best-positioned entities – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk."[2]

As previewed in the National Cybersecurity Strategy, the Implementation Plan sets out the Biden Administration's next steps in developing a cybersecurity strategy aimed at increasing public investments in cybersecurity across the public and private sectors, as well as harmonizing agency regulations governing companies' responses to cybersecurity incidents.

## Key Takeaways

- The NCSIP continues a cybersecurity agenda organized around five pillars: defense of critical infrastructure, disruption and dismantling of threat actors, shaping market forces to drive security and resilience, investments, and international partnerships.

- The initiative on cyber regulatory harmonization will include a request for information from the Office of the National Cyber Director to private sector stakeholders "to understand existing challenges with regulatory overlap and explore a framework for reciprocity for baseline requirements."[3]

- The federal government will pursue objectives to shift liability for insecure software products and services. Perhaps to acknowledge the uncertain prospects for legislation to establish a liability regime for software products and services, the NCSIP's modest proposal is for the Office of the National Cyber Director to host a symposium to begin exploring approaches to a new liability framework governing software.[4] CISA will advance efforts to develop a software bill of materials (SBOM), a form of inventory of software components.[5] Under the NCSIP, CISA will also "work to build domestic and international support for an expectation of coordinated vulnerability disclosure among public and private entities, across all technology types and sectors . . . ."[6]

- The NCSIP also indicates a push to impose cybersecurity-related rules across new industries. For example, the Department of Commerce will publish a Notice of Proposed Rulemaking to lay out requirements for Infrastructure-as-a-Service (IaaS) providers and resellers.[7]

- The Internet of Things (IoT) will also be a target of federal government attention, with the National Security Council tasked with drafting the contours of an IoT security labeling program and identifying an agency to lead regulatory efforts.[8] In a related development, on July 18 the White House also announced a "U.S. Cyber Trust Mark" program, in which the Federal Communications Commission (FCC) will establish a voluntary label for products that meet certain cybersecurity criteria.[9]

- The federal government will continue to marshal its procurement authority to encourage cybersecurity protections among government grantees and contractors and pursuing civil actions under the False Claims Act against grantees and contractors who knowingly provide deficient cybersecurity products or services, misrepresent their cybersecurity practices, or violate monitoring and reporting obligations.[10]

- Consistent with the government's all-tools approach to combatting cybercrime, the NCSIP includes initiatives for the Department of State, Department of Justice and FBI to disrupt ransomware threat actors, working in tandem with the Joint Ransomware Task Force.[11]

We will continue to provide updates on developments in cyber policy.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

**John P. Carlin**
+1-202-223-7372
jcarlin@paulweiss.com

**Jeannie S. Rhee**
+1-202-223-7466
jrhee@paulweiss.com

**Peter Carey**
+1-202-223-7485
pcarey@paulweiss.com

*Associate Matthew J. Disler also contributed to this Client Memorandum.*

---

1 *See* Paul Weiss Client Memorandum, *Biden Administration Announces Updated National Cybersecurity Strategy* (Mar. 13., 2023), https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/biden-administration-announces-updated-national-cybersecurity-strategy?id=46268.

2 The White House, "FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan" (July 13, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/.

3 NCSIP, Initiative No. 1.1.1.

4 NCSIP, Initiative No. 3.3.1.

5 NCSIP, Initiative No. 3.3.2; *see Software Bill of Materials*, CISA, https://www.cisa.gov/sbom.

6 NCSIP, Initiative No. 3.3.3.

7 NCSIP, Initiative No. 2.4.1.

8 NCSIP, Initiative No. 3.2.2.

9 The White House, "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers" (July 18, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/.

10 NCSIP, Initiative Nos. 3.5.1-2.

11 NCSIP, Initiative Nos. 2.5.1-4.