Updates
August 01, 2023
Cybersecurity Implementation Plan Offers a Roadmap for Cyber Priorities

The Biden Administration recently reaffirmed its continued focus on cybersecurity by announcing an Implementation Plan for the National Cybersecurity Strategy (the Plan).

The Plan provides a roadmap covering the policies and initiatives that the Administration intends to develop or update in advancing the five cybersecurity pillars that it announced in March: (1) defend critical infrastructure; (2) disrupt and dismantle threat actors; (3) shape market forces; (4) invest in a resilient future; and (5) forge international partnerships. Like the National Cybersecurity Strategy (the Strategy), it aims to ensure that the "biggest, most capable, and best-positioned entities"—both public and private—assume a greater share of the burden of mitigating cyber risk and driving long-term investments into cybersecurity. Private critical infrastructure operators, as well as public sector vendors, will need to be ready to bear that burden and take advantage of forthcoming government incentives.

As described below, the Plan reflects both the Administration's view that producers and suppliers must bear more responsibility for cybersecurity and its strategy of deconfliction and private-sector engagement. This combination brings potential costs and opportunities for industry, particularly in critical infrastructure, cloud service, and Internet of Things (IoT).

Cybersecurity Won't Be Built in a Day

Spanning more than 65 federal initiatives assigned to 18 different federal agencies, the Plan demonstrates that the Biden Administration appreciates the magnitude of its task. Each initiative is paired with a timeline for completion and maps to one of the Strategy's pillars and strategic objectives. While some initiatives establish broad cyber coordination imperatives (e.g., interagency harmonization and standards development) or are government facing (e.g., modernizing federal technology), others point to policies and capabilities that will involve and affect the private sector. The Administration's emphasis on using policy and regulation to correct

market failures signals that substantial impacts on industry are coming.

In particular, companies should heed the following initiatives.

- **New cybersecurity regulations.** The Plan offers a window into a future with increased cross-sector cybersecurity regulation. Whereas today cybersecurity regulations tend to either be generally framed (i.e., requirements for "reasonable security measures" in state omnibus privacy laws) or focused on discrete sectors, a number of initiatives contemplate new cyber regulations that cut across sectors. In particular, the Plan targets Q4 2025 to finalize the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which includes a 72-hour reporting window for incidents, for thousands of private operators across discrete sectors (on top of the web of state-level breach reporting obligations that apply today). The Plan further directs the National Security Council to work with regulators to propose new legal authorities for the government to affirmatively enforce cybersecurity requirements in critical infrastructure. At the same time, the Plan calls for collaboration with industry to harmonize and streamline cybersecurity regulation.
- **New and expanded liability regimes.** The Plan both highlights the government's short-term expansions of current liability regimes and proposes the creation of a new liability and safe harbor framework. In the short term, the U.S. Department of Justice (DOJ), through the Civil Cyber-Fraud Initiative, will increasingly apply the False Claims Act (FCA) against government grantees and contractors who do not meet their cybersecurity obligations or misrepresent their cybersecurity practices or protocols. In the longer term, the Office of the National Cyber Director will engage public and private stakeholders to explore different approaches to a liability framework for software products and services, as well as a safe-harbor framework to shield companies that securely develop and maintain their software products and services.
- **Broad public-private engagement.** The Plan outlines multiple opportunities for the private sector to engage with regulators and legislators as they develop new policies and requirements. In the near term, the Office of the National Cyber Director (ONCD) will publish a request for information regarding cybersecurity regulatory harmonization. Stakeholders will also have the opportunity to give input on proposed Know Your Customer requirements for Infrastructure-as-a-Service (IaaS) providers and resellers as part of a forthcoming Notice of Proposed Rulemaking and on draft rule changes to the Federal Acquisition Regulation (FAR) requirements for cybersecurity incident reporting and cybersecurity contract requirements.
- **New procurement obligations and funding opportunities.** The recommendations include using federal grants and procurement programs to promote cybersecurity research and development and to improve infrastructure cybersecurity. Operators that serve as federal contractors, or those that anticipate applying for federal grants, should anticipate stricter cybersecurity requirements within those contracts and grant awards. The government will also modernize its own technology infrastructure and update its lifecycle plans to enhance its security.

Across all five pillars, successful implementation will require cooperation and collaboration among the private sector, international partners, civil society, and all levels of the government. As the National Cybersecurity Strategy continues toward implementation, private operators (particularly those in critical infrastructure sectors) must prepare to assume a greater and more proactive role in U.S. cybersecurity. Given the breadth of cyber regulatory measures under consideration, operators should familiarize themselves with the Plan, both to assess the impact of the new regulations on their plans for current and future cybersecurity operations to ensure regulatory compliance and to identify early opportunities to engage with the agencies tasked with shaping those laws. And the potential for shifting liability upward provides an incentive for industry to help define the standard of care and ensure that it meets or exceeds that standard as it develops.

The Plan is the Biden Administration's latest move signaling an increased emphasis on cybersecurity outcomes (as opposed to checklist-based requirements) and on shifting responsibility and liability upstream from

consumers to producers. Companies should pay close attention to opportunities to help shape new regulatory and liability schemes and should also anticipate greater scrutiny of cybersecurity issues that affect customers and supply chains.

The authors wish to acknowledge Summer Associate Sydney Veatch's contributions to this Update.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response

Related insights

Update

The Biden Administration’s National Cybersecurity Strategy: Impact on the Private Sector

Update

CISA Seeks Input on New Cybersecurity Reporting Requirements