wiley

ALERT

New White House Policy Previews Increased Cybersecurity Oversight and Regulation

May 2, 2024

On April 30, 2024 the White House updated the foundational U.S. government policy that defines critical infrastructure (CI) sectors and establishes a coordination structure within the federal government to support owners and operators of CI in those sectors. The Administration's National Security Memorandum-22 on Critical Infrastructure Security and Resilience (NSM-22) replaces its predecessor document, Presidential Policy Directive 21 (PPD-21). The new policy keeps intact the general CI framework that was developed under PPD-21, including maintaining 16 CI sectors. However, NSM-22 represents a significant shift towards regulation of owners and operators of CI within these sectors, as it directs federal agencies to set "minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure."

Companies within one of the CI sectors – including Communications, Information Technology, Financial Services, Healthcare, and Transportation, among others – should be aware of this latest push for cybersecurity requirements and the federal regulatory activity that will likely flow from this new policy. This effort comes on the heels of DHS's proposed rules for mandatory cybersecurity incident reporting obligations for CI owners and operators, among other efforts to set requirements for these companies regarding security and resilience more generally.

The New Policy Previews Additional Regulation and Will Define "Systemically Important Entities"

The updated Biden Administration CI security and resilience policy moves forward on two major issues that CI companies should be aware of.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

- First, NSM-22 directs federal departments and agencies with regulatory authorities "to establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure." While this is not the first time that the Biden Administration has encouraged federal agencies to regulate CI companies, NSM-22 expands the scope of regulatory activity beyond cybersecurity to physical security and resilience. NSM-22 also encourages state, local, tribal, and territorial governments to establish minimum requirements for risk management, which could lead to further duplication and overlap between federal and other government requirements.
- Second, NSM-22 directs the Cybersecurity and Infrastructure Security Agency (CISA) to identify "***systemically important entities***" (SIEs), whose infrastructure, if disrupted or malfunctioning, would "cause nationally significant and cascading negative impacts to national security (including national defense and continuity of Government), national economic security, or national public health or safety." This mandate adopts a recommendation from the Cybersecurity Solarium Commission, as well as a requirement from a 2013 Executive Order. CISA must collaborate with other federal agencies who have responsibilities for particular CI sectors in developing the list of SIEs, and the list will not be made public. CISA has previewed that companies who are designated as SIEs would receive priority for information sharing and technical assistance from the federal government, but the designation will likely also come with increased regulatory expectations.

Most Critical Infrastructure Companies Will Not See a Change in Their Day-to-Day Interactions with Their Sector Risk Management Agencies

Apart from the regulatory focus and implementation of the SIE concept, NSM-22 is more of an evolution than a revolution. NSM-22 does not make large-scale structural or organizational changes to the existing federal model for CI security and resilience collaboration. The policy retains the PPD-21-assigned roles and responsibilities for federal agencies as "sector risk management agencies" (SRMAs), and it does not create new or modify the existing 16 CI sectors. The Administration did not adopt suggestions, including from a 2021 CISA report, to establish new sectors for space and the bioeconomy.

NSM-22 does make some modest changes to how the federal government will manage CI protection efforts. The policy clarifies and assigns additional coordination responsibilities for CISA and directs closer engagement between U.S. intelligence agencies and CI companies. CI owners and operators will have opportunities to identify sector intelligence needs and priorities that can support their security and resilience efforts.

Critical Infrastructure Companies Should Be Prepared for Increased Activity from Federal Agencies on Cybersecurity

NSM-22 will launch increased activity in the federal government related to cybersecurity. Most significantly, CI owners and operators should be prepared for potential new cybersecurity requirements, including from sector-specific regulators and through federal procurement. The new policy does not give significant details about what security and resilience minimum requirements might look like, but does point to "existing voluntary consensus standards" as a starting point. A look at recent cybersecurity requirements may be instructive, as

agencies such as the Federal Communications Commission (FCC) have begun to require select funding recipients to certify that they have cybersecurity and supply chain risk management plans based on voluntary National Institute of Standards and Technology (NIST) guidance.

Additionally, NSM-22 highlights the potential for adopting new requirements into federal procurement. The policy encourages federal agencies to use "grants, loans, and procurement processes, to require or encourage owners and operators to meet or exceed minimum security and resilience requirements," while also specifically tasking the General Services Administration with ensuring that "Government-wide contracts for critical infrastructure assets and systems [...] include appropriate audit rights for the security and resilience of critical infrastructure."

The new policy will kick off 13 separate implementation actions for federal agencies, including requiring SRMAs to issue sector-specific risk management plans. Of note, SRMAs are directed to consult with their sector coordinating councils in this effort, so there will be opportunities for industry engagement.

As with earlier moves from this Administration to pursue cybersecurity regulation, CI companies may want to take advantage of the SRMA structure and public comment opportunities to provide their expertise and experience in developing minimum security and resilience requirements that are flexible, outcome-based, and realistic.

Wiley's Privacy, Cyber & Data Governance team has helped companies of all sizes from various sectors proactively address risks and compliance with new cybersecurity laws and requirements. Please reach out to any of the authors with questions.