Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

July 25, 2024

The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience

The White House issued a directive, "National Security Memorandum on Critical Infrastructure Security and Resilience" (NSM-22), on April 30, 2024. The memorandum set forth a revised framework for federal agency roles and responsibilities within the national critical infrastructure risk management enterprise. The Secretary of Homeland Security is designated as the responsible official for coordination and implementation of NSM-22, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA) as the National Coordinator for the Security and Resilience of Critical Infrastructure. NSM-22 supersedes Presidential Policy Directive 21 (PPD-21), issued by President Barack Obama in 2013.

As the first comprehensive high-level policy guidance on critical infrastructure security and resilience (CISR) in more than a decade, NSM-22 presents an updated assessment of the broader strategic environment that is characterized by rapidly evolving, high complexity threats. NSM-22 envisions an accelerated risk management cycle for the CISR enterprise, requiring biennial updates of national infrastructure risk management plans from designated officials and agencies, as well as enhanced intelligence collection, analysis, and sharing. Additionally, it mandates a more assertive use of federal regulatory authorities and fiscal instruments, such as procurement and grant rules to encourage private-sector compliance with minimum resilience standards. As such, the directive shifts away from the policy approach first established during the Clinton Administration, which eschewed compulsory measures in favor of voluntary public-private partnerships to promote infrastructure resilience.

In some aspects, NSM-22 is restrained in scope. It retains PPD-21's sector-specific organization of the federal CISR enterprise, which is based on public-private partnerships organized within designated sectors that encompass wide areas of the economy and government (e.g., transportation, communications, energy). NSM-22 likewise preserves existing sector-specific coordination bodies and the leadership role of Sector Risk Management Agencies (SRMAs) for each of the 16 currently designated sectors. NSM-22 does not add any new sectors. (A Department of Homeland Security [DHS] 2022 report to Congress raised the possibility of adding new Space and Bioeconomy sectors.) Further, NSM-22 reiterates or reinstates many of the core concepts established by PPD-21 and other directives, such as the definitions of *critical infrastructure* and *risk*. NSM-22 places renewed policy emphasis on identification, cataloguing, and prioritization of specific assets within designated sectors, echoing the critical infrastructure protection policies of the Bush Administration after the terrorist attacks on September 11, 2001.

Strategic Context and Policy Approach

The White House framed NSM-22 in the context of several key developments: the "generational investment" in critical infrastructure; the transition of the national energy and transportation sectors away from fossil fuels; (unspecified) technological transformations; and increasingly interdependent and interconnected critical infrastructure in the modern economy.

PPD-21, by contrast, generally was more inward looking in its orientation, focusing on maturation of the modern homeland security enterprise that was little more than a decade old in 2013. It pivoted from the counterterrorism focus of the previous decade to broader engagement with an "all-hazards environment" of more diffuse and diverse challenges, including natural hazards. PPD-21 highlighted issues of interagency organization and coordination, information sharing, and analysis throughout the federal government, prioritizing development of interagency relationships and agency capabilities.

NSM-22 retains elements of the PPD-21 all-hazards approach and concern with interagency relationships and functions. However, much of NSM-22's content reflects emergence of threats not mentioned in PPD-21 (i.e., effects of climate change, supply chain disruptions, malign foreign investments in critical infrastructure entities, and more aggressive threats from nation-states with advanced cyber capabilities). NSM-22 generally refrains from re-imaginings of core concepts, institutions, and risk management methods. Instead, it directs federal agencies to mobilize for critical infrastructure protection and make use of existing authorities—and, if needed—seek new ones, stating that "federal departments and agencies with regulatory authorities shall utilize regulation, drawing on existing voluntary consensus standards as appropriate, to establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure."

Key Definitions and Concepts

In NSM-22, various key definitions and concepts developed in PPD-21 and other prior policy directives are restated, modified, or omitted.

Critical Infrastructure and Criticality

NSM-22 restates the definition of *critical infrastructure* used in PPD-21 as certain "vital" infrastructure objects, whose "incapacity or destruction would have a debilitating impact on national security, national economic security,

national public health or safety, or any combination of those matters." This definition of critical infrastructure was first introduced in statute under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act; P.L. 107-56) and has since been incorporated by reference into many subsequent laws and executive branch policy directives.

The PATRIOT Act definition presupposes an asset-centric approach to risk management based on the identification, prioritization, and protection of specific infrastructure assets deemed to meet the statutory threshold of criticality. A 2003 White House directive for critical infrastructure protection set forth "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources," based on the Patriot Act definition of critical infrastructure. Implementation of asset-level prioritization policies and legislative mandates encountered practical difficulties and criticism from oversight bodies over time. A decade later, PPD-21 contained few provisions for asset identification and prioritization activities, with no specific implementation requirements for this activity.

By contrast, NSM-22 instructs federal agencies to play a more direct and assertive role in public-private partnerships—both voluntary and regulatory—to identify, prioritize, and protect critical assets. The directive then incorporates this broad guidance into specific implementation instructions. NSM-22 provides a definition of criticality as "an attribute of an asset, system, or service that reflects its degree of importance or necessity to stated goals, missions or functions, or continuity of operations." It does not provide standardized metrics or detailed guidance to federal agencies for identification of priority assets on a national level through quantitative risk assessments or other means.

Risk

NSM-22 defines *risk* as "the potential for an unwanted outcome, as determined by its likelihood and the consequences"—a definition that DHS has used for more than a decade, sometimes presenting it as a mathematical function, where risk equals the product of threat, vulnerability, and (predicted) consequence. Some experts believe this formula has limited usefulness for quantitative comparisons of risk that might inform asset prioritization. NSM-22 seems to present the formula as a qualitative assessment approach; it nonetheless instructs agencies to use it for prioritization of risk management efforts.

National Critical Functions

In 2019, CISA introduced an analytical framework based on a set of 55 National Critical Functions (NCFs) intended to supplant "entity level risk management" based on asset-specific estimates of threat, vulnerability, and consequence. The NCF framework groups diverse infrastructure functions into four areas: connect, distribute, manage, and supply. It seeks to provide "a richer understanding of how entities come together to produce critical functions" by using a "functional lens" to understand critical infrastructure interdependencies across multiple sectors. NSM-22 does not mention the NCF framework, and its requirements for cross-sector risk assessments appear to be largely based on aggregation of sector-specific asset identification and prioritization inputs.

Key Implementation Milestones

Selected NSM-22 requirements include the following actions:

The Secretary of Homeland Security (the Secretary) produces the National Infrastructure Risk Management Plan (within one year, recurring biennially) as the government's "comprehensive plan to mitigate and manage cross-sector risk"; acting through CISA, creates the national coordinator office to act as "the single coordination point for SRMAs across the Federal Government"; and reviews the existing CISR framework for public-private partnerships and recommends necessary changes (within one year).

SRMAs designate a senior official (within 30 days) to coordinate SRMA functions and stakeholder engagements within their respective sectors; provide a detailed justification of selection criteria, agency support, and mission fulfilment plans (within 180 days); and produce a sector-specific risk management plan (within 270 days, recurring biennially).

SRMAs and the national coordinator review "available authorities, incentives, and other tools to encourage and require owners and operators to implement identified sector-specific or cross-sector minimum security and resilience requirements" and propose "any additional authorities or capabilities that could enable implementation" (within 270 days).

The national coordinator produces a list (no timeline) of *Systematically Important Entities* that could cause cascading infrastructure failures on a national scale based on SRMA identifications of prioritized infrastructure assets and certain other inputs.

The director of national intelligence (DNI) provides an intelligence estimate to the President on critical infrastructure threats (within 180 days); provides reports on intelligence collection (within one year, recurring annually) and information sharing with SRMAs and critical infrastructure entities (within 18 months, recurring annually); and provides guidance (within one year) on timely threat notification to designated federal agencies of specific and credible threats to U.S. critical infrastructure.

Issues for Congress

The next Administration may rescind, modify, or fully implement NSM-22 without congressional action. Congress may legislate changes to federal CISR policy. In the 118th Congress, some Members have introduced bills to create a Space infrastructure sector, to establish a national risk management process based on the NCF framework, and to require certain threat and vulnerability assessments.

Brian E. Humphreys, Analyst in Science and Technology Policy

Disclaimer