




Homeland Security

June 14, 2024

MEMORANDUM FOR DISTRIBUTION

FROM: Alejandro N. Mayorkas
Secretary

SUBJECT: Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025)



In accordance with my responsibilities outlined in the National Security Memorandum-22 on *Critical Infrastructure Security and Resilience* (NSM-22), I am pleased to issue this strategic guidance for improving the security and resilience of our nation's critical infrastructure, including priorities to guide our shared efforts throughout the 2024-2025 national critical infrastructure risk management cycle established in NSM-22.

In this era of technological advancements and dynamic global volatility, the security and resilience of our critical infrastructure are of paramount importance. Energy grids, water and wastewater systems, transportation networks, healthcare facilities, communication networks, and other essential systems are vital for public safety, economic security, and national security. The increasing interconnectivity of critical infrastructure systems and reliance upon global technologies and supply chains make these systems susceptible to a myriad of threats. Recent threat assessments, including the *2024 Homeland Threat Assessment*, identify potentially disruptive cyberattacks, physical sabotage, climate change, and geopolitical tensions among the greatest risks that we face. As those of us responsible for the security and resilience of U.S. critical infrastructure navigate this increasingly complex risk landscape, we must collectively address emergent risks and an uncertain future while remaining vigilant against longstanding threats like terrorism, cyber espionage, and targeted violence.

In NSM-22, the President established a two-year risk management cycle that prioritizes the identification and mitigation of critical infrastructure risk at the asset, sector, and national levels. Addressing these risks will require a coordinated effort by DHS, Sector Risk Management Agencies (SRMAs), and other relevant Federal agencies; state, local, tribal, and territorial (SLTT) governments; infrastructure owners and operators; and other stakeholders across the critical infrastructure community both domestic and abroad. The forthcoming sector-specific risk management plans and the first biennial National Infrastructure Risk Management Plan represent an opportunity to communicate to all critical infrastructure stakeholders how the U.S. government will prioritize risk management efforts over the next two years.

Priority Risk Areas

To address a range of emergent and complex risks, we must build upon existing models of public-private partnership and work toward meaningful operational collaboration. In so doing, efforts of the critical infrastructure community should prioritize the following five priority risk areas. While these priorities vary in complexity and familiarity and will require different levels of engagement across the various sectors, SRMAs should address these risks as part of their efforts to implement NSM-22, including through engagement, bi-directional information sharing, and enhanced collaboration with industry through existing Information Sharing and Analysis Centers (ISACs), Sector Coordinating Councils (SCCs), and Government Coordinating Councils (GCCs).

- ***Address cyber and other threats posed by the People’s Republic of China (PRC)***—The U.S. Intelligence Community has provided public warnings about the PRC’s capability to launch cyberattacks on U.S. critical infrastructure and its willingness to target defense critical infrastructure (DCI) and other key critical infrastructure systems and assets to achieve its long-term strategic objectives. We also face threats from other malign “gray zone” activities, to include financial investments in infrastructure and emerging technologies, traditional espionage, and insider threats. Attacks targeting infrastructure essential to protect, support, and sustain military forces and operations worldwide or that may cause potential disruptions to the delivery of key goods or services to the American people must be our top priority. Leveraging timely and actionable intelligence and information and adopting best practices for security and resilience, SRMAs, critical infrastructure owners and operators, and other SLTT and private sector partners shall devise and implement effective mitigation approaches to identify and address threats from the PRC, including plans to address cross-sector and regional interdependencies. SRMAs should also support cross-sector risk management and the Department of Defense’s DCI resilience efforts. DHS will collaborate with government and private sector partners to develop plans and capabilities to manage consequences of complex incidents involving critical infrastructure, including a National Security Emergency Plan and updated National Cyber Incident Response Plan, and to strengthen intelligence and information sharing across the community. Capacity building efforts to address the PRC threat will increase the security and resilience of our infrastructure against other state and non-state sponsored actors.
- ***Manage the evolving risks and opportunities presented by Artificial Intelligence (AI) and other emerging technologies***—We must continue to proactively address AI as a transformative and general-purpose technology and consider the implications of other emerging technologies on critical infrastructure. As directed in Executive Order 14110 on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, SRMAs developed their first critical infrastructure AI annual risk assessments and DHS developed Safety and Security Guidelines for Critical Infrastructure Owners and Operators. DHS has also provided guidance regarding the emergence of cryptographically relevant quantum computers in the coming years that pose risks for sensitive data maintained by critical infrastructure entities. SRMAs and critical infrastructure owners and operators should integrate relevant risk assessments and DHS guidance into their sector-specific risk assessments and sector-specific risk management plans to address risks from AI and other emerging technologies. While we must look to mitigate new risks, we must also recognize that new AI-enabled systems and other emerging technologies will also provide new tools to

help mitigate threats to critical infrastructure. SRMAs should identify, and where possible pilot or deploy, AI and other technology-informed risk mitigation tools to increase the security and resilience of critical infrastructure against other threats considering the National Institute of Standards and Technology (NIST) AI Risk Management Framework and relevant DHS guidance.

- ***Identify and mitigate supply chain vulnerabilities***—The nation faces increasing threats to the resilience of supply chains for essential goods and services. The COVID19 pandemic showed the consequences of offshoring significant parts of critical supply chains and the need to reemphasize resilience alongside efficiency as part of the preparation for future public health and other crises. We have seen potential for other significant supply chain disruptions related to potential rail strikes and physical attacks on vessels in the Red Sea. Expanding visibility into shared internationally systemic risks is also important in order to fully understand, manage, and reduce risk to U.S. critical infrastructure, including implications of relying on state-owned enterprises and suppliers from foreign adversaries. The resilience of the nation’s civilian and military supply chains is a matter of national and homeland security. Executive Order 14017 on *America’s Supply Chains* began the process to rebuild and revitalize resilient American supply chains. DHS established the Supply Chain Resilience Center to lead and coordinate the Department’s effort to assess and mitigate potential supply chain disruptions. DHS will work with SRMAs, other relevant Federal agencies, critical infrastructure owners and operators, and other experts to identify goods, services, or components most vulnerable to supply chain disruption and seek to mitigate the effects of supply chain disruptions for essential systems.
- ***Incorporate climate risks into sector resilience efforts***—Executive Order 14008 on *Tackling the Climate Crisis at Home and Abroad*, elevated climate considerations to be an essential element of U.S. national security. Intensifying threats from climate change to our nation’s critical infrastructure include extreme cold and heat, flooding, drought, sea-level rise, thawing permafrost, and wildfires in addition to the increased frequency and severity of hurricanes and other storms. Historic investments in rebuilding and protecting infrastructure against these threats through the Infrastructure Investment and Jobs Act are making the nation’s critical infrastructure more sustainable and resilient. DHS and SRMAs must work with others in the Executive Branch to ensure that these investments are leveraged to continue to build resilience of critical infrastructure against all hazards and that our critical infrastructure security and resilience efforts remain focused on climate-related risks.
- ***Address growing dependency of critical infrastructure on space systems and assets***—Technology has advanced to the point that access to space-based services, like the Global Positioning System (GPS) and satellite communications, is taken for granted across critical infrastructure. While these services are efficient and beneficial, dependence on space systems can introduce risk. Russia’s cyberattacks in 2022 against commercial satellite communications networks as part of its invasion of Ukraine illustrate the importance of protecting such infrastructure from malicious adversaries. Space debris also poses a potential risk to critical space systems and assets. While there is no designated space critical infrastructure sector, the National Space Policy and the United States Space Priorities Framework articulate the U.S. government’s responsibility for protecting and securing space-related systems and assets. SRMAs and critical infrastructure partners should prioritize

assessing their reliance on space systems and assets and the potential cascading impacts on their sector if disruptions were to occur. DHS, in coordination with SRMAs and relevant private sector partners, will expand efforts of the Space Systems Critical Infrastructure Working Group to prioritize and mitigate space-related risks to critical infrastructure.

Priority Risk Mitigations

To address and manage these and other risks, critical infrastructure stakeholders must adopt risk mitigation efforts that can accomplish results at scale. We must collectively prioritize mitigations that reduce the frequency—and more importantly the consequences—of adverse incidents when they occur. We must thus focus on the following all-hazards priority risk mitigations:

- ***Build resilience to withstand and recover rapidly from all threats and hazards***—Resilience within and across critical infrastructure sectors is essential to ensure the delivery of goods and services to the American people and avoid disruptions to essential government functions. The President’s Council of Advisors on Science and Technology (PCAST) recently stressed that “we cannot make all our infrastructure impervious to every threat or hazard” and “[i]nstead, we must make our cyber-physical infrastructure resilient.” While we cannot keep determined advanced persistent threats or ransomware actors completely at bay or prevent severe weather occurrences, we can minimize the consequences of incidents by understanding critical nodes, assessing dependencies within systems, and developing plans to ensure rapid recovery. SRMAs, in coordination with DHS and other relevant Federal agencies, should work with owners and operators of critical infrastructure to develop and adopt resilience measures, anticipate potential cascading impacts of adverse incidents, and devise response plans to quickly recover from all types of shocks and stressors.
- ***Adopt security and resilience baseline requirements***—Individual critical infrastructure owners and operators must be encouraged by SRMAs and, where applicable, held accountable by regulators for implementing baseline controls that improve their security and resilience to cyber and all hazard threats. Establishing minimum cybersecurity requirements as part of these efforts to secure critical infrastructure also aligns with the 2023 National Cybersecurity Strategy. SRMAs and other relevant Federal and SLTT government agencies must also look to grant making capabilities, procurement powers, and other authorities to incentivize and enforce the implementation of minimum all-hazards, including cyber, security and resilience requirements across critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs) and the NIST Cybersecurity Framework 2.0 are good examples of existing tools that provide a common set of protections against threats, such as ransomware. DHS will work with SRMAs, regulators, and private sector entities to ensure that baseline requirements are risk-informed, performance-based, and to the extent feasible, harmonized and to develop tools that support the adoption of such requirements.
- ***Incentivize service providers to drive down risk at scale***—Increasingly, critical infrastructure owners and operators are dependent on the providers of shared infrastructure, products, or services. While such shared services and products can bring significant benefits, they can also result in unique risks or the concentration of risk in vendors who malicious actors are not hesitant to target. For example, in December 2023, Iranian actors took advantage of the

widespread use of a programmable logic controller with a default password across the Water and Wastewater Systems Sector. The Cyber Safety Review Board also recently issued a report looking at compromises in major cloud service offerings with broad implications for customers, while also offering concrete security recommendations. DHS must work with critical infrastructure vendors and providers of shared services and infrastructure to ensure that products and services are deployed with security built in. Driving secure-by-design principles can reduce the cybersecurity burden on small to mid-sized businesses. DHS and SRMAs must continue to engage with relevant stakeholders to understand the risks associated with legacy infrastructure, hardware, or services and how vendors can ensure that new products and services are deployed in a way that increases security and resilience.

- ***Identify areas of concentrated risk and systemically important entities***—As CISA coordinates with SRMAs to identify sector, cross-sector, and nationally significant risk, we must identify and prioritize systemically important entities to inform the government’s ability to manage risk. We must thus work to develop a greater understanding of dependencies and interdependencies within and across sectors. The Water and Wastewater Systems Sector, for example, is dependent on the Chemical Sector for water purification and sanitation. And nearly all sectors rely on the energy generated and transmitted by the Energy Sector to deliver essential goods and services. As the recent ransomware attack on a major health insurer demonstrated, there can also be previously unknown or underappreciated concentration of risks within a particular sector. In that incident, the disruption of a single provider resulted in widespread impact on the ability of Americans to obtain medical prescriptions. SRMAs must better understand where risks in their sector may be concentrated to inform sector and cross-sector risk mitigation efforts and the identification of systemically important entities.

National Coordinator

As the National Coordinator for the security and resilience of critical infrastructure, the CISA Director will drive efforts by SRMAs, other Federal Departments and Agencies, owners and operators, and others in the critical infrastructure community to address these priority risks and adopt priority risk mitigation activities on my behalf including through the Federal Senior Leadership Council and appropriate SCCs and GCCs. The priorities identified above will be addressed as part of the National Infrastructure Risk Management Plan, which will replace the 2013 National Infrastructure Protection Plan, and should be specifically included in each sector-specific risk assessment and in all sector-specific risk management plans. Additional guidance on the content and format for the sector-specific risk assessments and sector-specific risk management plans will be provided by the National Coordinator under separate cover.

Under NSM-22, building secure and resilient critical infrastructure is a shared responsibility. I invite all SRMAs, other Federal and SLTT entities, and private sector partners to join in this concerted effort managing prioritized risks and mitigations to effectively protect our critical infrastructure and national security.