CSC 2.0

Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure

Mary Brooks, Annie Fixler & RADM (Ret.) Mark Montgomery

Executive Summary

Few things more directly impact Americans' security and well-being than the reliability, availability, and safety of critical infrastructure. The security of this critical infrastructure relies, in turn, on the strength of the relationship between the government and the private sector, which owns and operates the majority of the infrastructure. Thus, the federal government has endeavored for decades to build a strong relationship with the private sector.

Nevertheless, the policy underpinning this public-private sector relationship has become outdated and incapable of meeting today's demands. Similarly, the implementation of this policy — and the organization, funding, and focus of the federal agencies that execute it — is inadequate. This report will evaluate the state of the public-private sector relationship and offer recommendations to reshape it to improve national security going forward.

The timing could not be better. In late 2022, the Biden administration announced its intention to rewrite the Obama-era Presidential Policy Directive 21 (PPD-21), which established the current iteration of the critical infrastructure protection framework. This decision followed congressional intervention two years earlier to clarify and expand the role of federal agencies responsible for interfacing with the private sector.[1] Congress designated these organizations as Sector Risk Management Agencies (SRMAs) — there is at least one for each of the 16 sectors of U.S. critical infrastructure. It also ordered the Department of Homeland Security (DHS) to review the SRMAs' performance and recommend improvements.

Before deciding to revamp PPD-21, the Biden administration conducted assessments of the federal government's authorities to regulate security standards for critical infrastructure[2] and launched a number of targeted, high-visibility efforts to address sector-specific problems and draw attention to cybersecurity issues. Additionally, the Biden administration has issued executive orders and national security memoranda intended to strengthen federal cybersecurity and lay out voluntary cybersecurity performance goals for critical infrastructure providers. The administration also established congressionally mandated public advisory committees to evaluate critical infrastructure protection.[3] The creation of the Office of the National Cyber Director, meanwhile, has provided improved strategic coordination across the interagency and with private sector stakeholders.

This incremental approach, however, is not delivering the necessary improvements to SRMA performance, especially as both physical and — especially — cyber threats to the country's critical infrastructure continue to escalate.

As the administration begins its review process, it should focus specifically on improving the relationship between the public and private sectors — by making government a better partner to industry and through both voluntary partnerships and regulation, as noted in the new National Cybersecurity Strategy.[4] This report identifies flaws in both the design and implementation of public-private collaboration policy and argues that these flaws are amplified by discrepancies in the structure, resourcing, and capabilities of SRMAs. In short, the performance of SRMAs is inconsistent at best and wholly deficient at worst.

Meanwhile, there are numerous other challenges. The strategy and policy documents governing critical infrastructure have become stale. The current systems for designating sectors as critical and for mitigating cross-sector risks are inadequate. DHS's Cybersecurity and Infrastructure Security Agency (CISA) is unable to fulfill its responsibilities, and it does not receive the interagency support necessary to act effectively as the national risk manager. Voluntary security relationships are not delivering the necessary results. Additionally, processes for sharing information, responding to emergencies, designating priority infrastructure within sectors, and promoting resilience are insufficient.

Despite these challenges, this report concludes that the overall concept underlying the government's critical infrastructure protection system — anchored in an approach that balances regulation, incentivization, and collaboration — remains the best method to coordinate the public and private sectors. The report offers operational-level recommendations to improve the existing system while addressing broader strategic considerations that require an update to PPD-21. It also offers specific guidelines on how to revise PPD-21 to preserve what is working while also addressing the significant challenges in building effective public-private collaboration.

Recommendations

Rewrite PPD-21 for a New Era

1. Clearly identify strategic changes
2. Assign responsibilities and ensure accountability for routine updates of key strategic documents
3. Clarify CISA's roles and responsibilities as national risk management agency (NRMA)
4. Resolve questions around the organization and designation of critical infrastructure sectors and assigned SRMAs
5. Provide guidance on SRMA organization and operation
6. Facilitate accountability

Support the PPD-21 rewrite with implementation and resourcing efforts

7. Strengthen CISA's capabilities to execute its NRMA responsibilities
8. Resource SRMAs for their responsibilities
9. Identify a more effective way to catalog, support, and protect priority infrastructure
10. Develop functional information-sharing capacity across all sectors
11. Organize public-private collaboration to mitigate systemic and cross-domain risk
12. Ensure effective emergency response

1. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, §9002(c), 116th Congress (2021). (https://www.congress.gov/bill/116th-congress/house-bill/6395)

2. Tim Starks, "The Biden National Cyber Strategy is Unlike Any Before It," *The Washington Post,* January 6, 2023. (https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it)

3. See, for example, CISA Cybersecurity Advisory Committee, "Report to the CISA Director: Building Resilience and Reducing Systemic Risk to Critical Infrastructure," September 13, 2022. (https://www.cisa.gov/sites/default/files/publications/CSAC_SR_September_2022_Final_Recommendations_09132022-508.pdf)

4. The White House, "National Cybersecurity Strategy," March 2023. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission
For more information, visit **www.CyberSolarium.org**