CSC 2.0

2024 Annual Report on Implementation

Jiwon Ma & RADM (Ret.) Mark Montgomery

Executive Summary

The cyber threat to America's national critical infrastructure has expanded since the U.S. Cyberspace Solarium Commission (CSC) issued its original March 2020 report. The threat comes from both nation-state adversaries, such as the Volt Typhoon attacks from China, and from criminals, who are escalating ransomware attacks, with a 74 percent increase in the number of reports in 2023. The vulnerabilities inherent in our highly networked infrastructures amplify the risk posed by such threats.

To date, about 80 percent of the Commission's original 82 recommendations have been fully implemented or are nearing implementation, and an additional 12 percent are on track to be implemented, a testament to the concerted efforts of the executive branch and Congress in the cybersecurity domain. While most of these recommendations were accomplished through legislation or policies similar to those suggested by the Commission, others were addressed, or are being addressed, by the administration or Congress using innovative solutions not initially considered by the Commission. This adaptability and creativity are commendable and further enhance the outcomes.

The executive branch leads the effort to achieve a unified cyber defense against malign cyber actors and establish deterrence in cyberspace. The Office of the National Cyber Director (ONCD), now led by the second Senate-confirmed national cyber director, Harry Coker, Jr., has been a key force in leading the development and implementation of a whole-of-government approach to cybersecurity policies. Administration efforts include:

- The ONCD completed 33 of the 36 initial initiatives to implement the National Cybersecurity Strategy published in March 2023.
- The White House issued a new national security memorandum on critical infrastructure security and resilience (NSM-22), creating a national risk management cycle.
- NSM-22 appointed the Cybersecurity and Infrastructure Security Agency (CISA) as the National Coordinator for the security and resilience of critical infrastructure and mobilized sector risk management agencies to better support private sector partners.
- Under Director Jen Easterly, CISA's capacity continues to increase, with a budget nearly double in size over five years.
- CISA has improved public-private integration efforts, mostly through the Joint Cyber Defense Collaborative (JCDC).
- The State Department's Bureau of Cyberspace and Digital Policy (CDP), under its inaugural leader, Ambassador-at-Large Nathaniel Fick, has advanced U.S. interests through cyber diplomacy and cyber capacity building for allies and partners.
- CDP published the first U.S. International Cyberspace and Digital Policy Strategy in May 2024.

On the legislative front, Congress has strengthened the foundations of cybersecurity in the private sector and within federal agencies. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) mandates that critical infrastructure entities report significant cyber incidents to CISA. CISA is now in the final rulemaking process to implement congressional intent.

Congress has also provided the executive branch with increased resources to address cybersecurity challenges facing the federal government, the U.S. military, and the private sector. The fiscal year (FY) 2024 omnibus spending bill, for example, appropriated a much-needed $2.8 billion for CISA and $22 million for the ONCD. The funding for sector risk management agencies, however, has been inconsistent, reflecting a failure of some federal agencies to recognize their responsibilities and request appropriate funding to support interagency efforts and collaborate with critical infrastructure owners and operators. To improve coordination and address funding disparities, in July 2024, the ONCD and the Office of Management and Budget (OMB) issued a joint memorandum outlining the administration's FY26 cybersecurity priorities to modernize technology, enhance public-private collaboration, combat cybercrime, and strengthen the cyber workforce while preparing for emerging threats and expanding global partnerships.

2024 Annual Report on Implementation

Jiwon Ma & RADM (Ret.) Mark Montgomery

The private sector is indispensable not only in securing its own networks but also in working with the federal government on cybersecurity policy development and implementation. Private sector participation in initiatives like the JCDC and the U.S. Cyber Trust Mark, a voluntary software labeling program for Internet of Things devices, will be key in guiding consumer choices and promoting manufacturer accountability for creating secure products. Additionally, private sector investments are supporting and shaping cybersecurity workforce and education policies, creating a more diverse workforce.

While significant progress has been made, more work needs to be done. Increasing cyber incidents targeting America's critical infrastructure sectors, like water and wastewater, aviation, and space, underscore the need for vigilance and robust defensive measures. This year's assessment includes recommendations of what the next Congress and administration should prioritize.

The Biden administration, Congress, and private sector leaders have followed the path charted by the Cyberspace Solarium Commission to defend U.S. national security and economic prosperity in cyberspace. Collectively, these efforts are improving layered cyber deterrence — a critical national security endeavor. We urge readers to consider this report as a way to gauge America's collective efforts while identifying areas where additional initiatives and deeper partnerships are necessary to improve national cyber resilience.

Senator Angus King (I-ME)
Co-Chair
CSC 2.0

Representative Mike Gallagher (R-WI)
Co-Chair
CSC 2.0

Top 10 Recommendations for the Incoming Administration and Congress

1. **Designate Benefits and Burdens for Systemically Important Entities (5.1)**
2. **Conduct Robust Continuity of the Economy Planning (3.2)**
3. **Codify Joint Collaborative Environment for Threat Information Sharing (5.2)**
4. **Strengthen an Integrated Cyber Center Within CISA (5.3)**
5. **Develop Cloud Security Certification (4.5)**
6. **Establish a Bureau of Cyber Statistics (4.3)**
7. **Establish Liability for Final Goods Assemblers (4.2)**
8. **Develop Cybersecurity Insurance Certifications (4.4)**
9. **Establish National Guard Cybersecurity Roles (3.3.6)**
10. **Build Societal Resilience Against Cyber-Enabled Information Operations (3.5)**

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**