2024 Annual Report on Implementation

Jiwon Ma & RADM (Ret.) Mark Montgomery

Top 10 Recommendations for the Incoming Administration and Congress

1. Designate Benefits and Burdens for Systemically Important Entities (5.1)
Prioritization among various critical infrastructure assets is imperative since the United States cannot protect everything, everywhere, all at once. Through NSM-22, President Biden tasked CISA with working with the other sector risk management agencies to identify systemically important entities (SIEs) within each critical infrastructure sector that have a disproportionate impact on U.S. national security, economic security, and public health and safety. NSM-22, however, does not outline the benefits and burdens for companies identified as SIEs, a key component of the CSC's initial recommendation on systemically important critical infrastructure. The next administration and Congress should work together to detail the intelligence and information-sharing benefits and the minimum cybersecurity burdens of SIEs.

2. Conduct Robust Continuity of the Economy Planning (3.2)
A national Continuity of the Economy (COTE) plan is essential for restoring critical economic functions in the event of a significant cyber disruption or other natural or manmade disaster. Developing a COTE plan requires gaining comprehensive insights through cyber threat intelligence, national-level tabletop exercises, and stakeholder engagements with the private sector and critical infrastructure owners. Although the FY21 National Defense Authorization Act (NDAA) authorized the development of a COTE plan, the report that the administration belatedly delivered to Congress in August 2023 dismissed the need for additional COTE planning. The report brushed aside gaps in current federal incident response capabilities and failed to grapple with the ways the private sector must participate in the development and implementation of the plan. Fortunately, the next administration will have a chance to reassess the prior report since the legislation mandating the original COTE plan requires updates every three years.

3. Codify Joint Collaborative Environment for Threat Information Sharing (5.2)
The joint collaborative environment's (JCE's) advanced integrative platform would facilitate real-time sharing and analysis of cyber threat intelligence among government agencies, private sector entities, and international partners. CISA's JCDC has driven forward the concept of a JCE. However, JCDC planning and coordination efforts typically involve fewer than 20 organizations and require additional legal authorities and a platform like the JCE to scale up its work. Private partners will play a crucial role in feeding information into the JCE, while federal agencies provide the structure for sharing data and analytical insights. The next administration and Congress need to codify JCE into law and ensure sustained funding for it.
Once established, the JCE will require data privacy and legal protection measures to safely share intelligence information among participants.

4. Strengthen an Integrated Cyber Center Within CISA (5.3)
Establishing an integrated cyber center (ICC) within CISA is essential to achieving a unified national defense against cyber threats. Currently, national cyber defense capabilities are fragmented across various federal agencies. For example, delays and inefficiencies in the response to the SolarWinds hack in 2020 highlighted the need for improved coordination between agencies like the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and CISA. Similarly, the May 2021 Colonial Pipeline ransomware attack demonstrated the need for a centralized approach to handle such incidents effectively. In addition to centralizing expertise and capabilities within CISA and empowering it as the nation's civilian cyber defense agency, the ICC would serve as a hub, standardizing response mechanisms and reducing redundancy and resource waste. As recommended by the Commission, the ICC would leverage specialized skills and insights from various federal agencies. For instance, the FBI would offer investigative capabilities, the NSA would provide intelligence insights, and CISA could provide its technical and homeland-specific cyber expertise. The ICC can also serve as a focal point for public-private collaboration by building on CISA's existing partnerships and information-sharing channels.

5. Develop Cloud Security Certification (4.5)

The widespread adoption of cloud computing by government agencies and critical infrastructure owners and operators should be a net positive for cybersecurity due to the deeper expertise in network security that cloud service providers can offer. However, recent years have seen dramatic failures by cloud providers to maintain a culture of cybersecurity and include cybersecurity services in their baseline offerings. In these cases, malicious actors have accessed unclassified government networks and critical infrastructure through cloud platforms. Currently, the United States lacks a standardized approach to securing the federal cloud infrastructure. While the FY23 NDAA authorized the Federal Risk and Authorization Management Program (FedRAMP) to standardize security assessment of cloud computing products and services for unclassified federal information, the program does not explicitly enforce cybersecurity standards through a security certification or other mechanisms. In addition to addressing these FedRAMP issues, the government should recognize and designate cloud service providers as a critical infrastructure. This designation, as recommended by the Commission, would either classify cloud services as a stand-alone critical infrastructure sector or, at least, as a unique sub-sector within the information technology sector. Appointing a sector risk management agency for oversight and management of cloud service providers can further mitigate risks.

6. Establish a Bureau of Cyber Statistics (4.3)

Currently, policymakers rely on outdated, incomplete, and inaccurate data on cybersecurity to make strategic decisions. In its March 2020 report, the Commission recommended establishing a Bureau of Cyber Statistics to serve as the federal statistical agency for collecting, analyzing, and disseminating cybersecurity data. The next administration should work with Congress to establish this bureau, ensuring it adheres to the standards and requirements set forth by the existing national statistical agencies and enables the secure curation of holistic data reflective of today's cybersecurity landscape. The Bureau could initially utilize data from federal agencies, such as data collected by CISA as mandated by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Additionally, the sector-based risk assessments required by NSM-22 would further support access to standardized data. Coordination with academia and the private sector would also facilitate the sharing of insights and best practices, enhancing the bureau's ability to inform cybersecurity strategies.

7. Establish Liability for Final Goods Assemblers (4.2)

Establishing liability for final goods assemblers will hold manufacturers accountable for cybersecurity breaches that exploit vulnerabilities in their products, incentivizing them to develop products that are secure from the outset. The liability framework would not only enhance product security but also ensure industry-wide improvements by requiring manufacturers to conduct thorough security testing before products reach consumers. While the ONCD has begun efforts to develop a flexible software liability framework, the effort is still nascent. Meanwhile, in a complementary effort, the Federal Communications Commission has finalized rules for its voluntary labeling program for consumer Internet of Things devices, known as the U.S. Cyber Trust Mark program. However, implementing liability requirements will require legislative action and a flexible regulatory framework. These should define manufacturers' responsibilities, conditions for liability, and penalties for non-compliance. Establishing these frameworks will promote transparency, accountability, and a culture of security across the technology industry, ultimately bolstering national security.

8. Develop Cybersecurity Insurance Certifications (4.4)

The current cyber insurance market is volatile, and too few companies have the coverage they need at premiums they can afford. In June 2024, Kimberly Denbow, vice president of the American Gas Association, warned that gas utilities are struggling with a limited "number of insurance providers willing to write cyber insurance policies." Four years ago, the Commission recommended that the Department of Homeland Security fund a federally funded research and development center (FFRDC) to research the insurance industry and help insurers find ways to offer better coverage that meets various sector-specific needs. Congress and the Biden administration have done little on this front even as the need for such an FFRDC has only grown. As originally envisioned by the Commission, the FFRDC would also work with the private sector and state insurance regulators to develop certification frameworks for cybersecurity insurance products as well as cyber insurance-related training models for underwriters and claims adjusters.

9. Establish National Guard Cybersecurity Roles (3.3.6)

The National Guard's unique position bridging the military and civilian sectors, as well as federal and state government authorities, makes it ideally suited to respond to domestic cyber threats. The 54 Guard entities have the local presence and capabilities that position them well to serve as a rapid response force for cyber incidents at both the state and federal levels. Over the years, the Guard has taken on more cybersecurity responsibilities and built more cyber capacity with specialized training and initiatives like the annual Cyber Shield exercise. Additionally, the Guard has participated in numerous state-level cybersecurity efforts. Building increased interoperability between CISA and the Guard could drastically improve the nation's speed and agility in responding to cyberattacks. However, increasing the cybersecurity response planning responsibilities of the Guard would require multiple facilitating actions from the incoming administration and Congress. Congress should assess how to integrate the Guard more effectively into executive branch cyber response planning efforts like the Department of Homeland Security's National Cyber Incident Response Plan (NCIRP) and state governor-directed cyber response and recovery operations. To achieve this integration, the next administration and Congress need to determine the Guard's long-term role in the cyber protection of critical infrastructures and identify the necessary authorities and resources to do this. It is also critical to issue guidance detailing the Guard's responsibilities, as well as those of CISA and the FBI, in collaboration efforts during incidents.

10. Build Societal Resilience Against Cyber-Enabled Information Operations (3.5)

Cyber-enabled malign influence operation campaigns pose a significant threat to the United States by undermining democratic processes, eroding public trust, and exacerbating social divisions. Enhancing public awareness through digital literacy educational programs is crucial for all age groups in countering these malign efforts. This year, several grants funded through the American Rescue Plan Act of 2021 and the bipartisan Infrastructure Investment and Jobs Act of 2021 have created digital literacy programs at the state level. While these programs are a step forward, the Commission recommends that Congress task the Department of Education, Department of Homeland Security, National Science Foundation, and the National Institute of Standards and Technology with developing curriculums focused on critical thinking and fact-checking skills, equipping citizens to identify disinformation and foreign influence. A successful curriculum would integrate social media literacy into K-12 lesson plans and promote adult education programs on digital citizenship. Investments in civic education are also essential. The next administration should request and Congress should appropriate increased funding for civic education to support these efforts to counter foreign malign influence operations.

CSC 2.0

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Mike J. Gallagher, Former U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Chris Inglis, Former National Cyber Director

Jim Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Ben Sasse, Former U.S. Senator for Nebraska

Suzanne Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partners

FDD