2023 Annual Report on Implementation

Jiwon Ma & RADM (Ret.) Mark Montgomery

Executive Summary

In the three years since the publication of the Cyberspace Solarium Commission's (CSC's) March 2020 report, both the executive and legislative branches have taken significant steps to improve the government and the nation's cybersecurity. In fact, nearly 70 percent of the recommendations in the initial CSC report have been implemented or are nearing implementation. But America's cyber adversaries have been busy in the intervening three years. Russia and China have conducted significant espionage attacks on the U.S. government and industries and have reportedly embedded malware in U.S. critical infrastructure to facilitate future nefarious activity. Criminal actors have also expanded both ransomware and cyber theft activities. We cannot afford to pause in the pursuit of enhanced cybersecurity.

Lawmakers have remained industrious on cybersecurity issues, both authorizing more cybersecurity programs and ensuring these initiatives have the resources critical to their success. At the end of last year, for example, Congress codified the new State Department's Bureau of Cyberspace and Digital Policy, which will promote responsible state conduct in cyberspace and advance U.S. interests. Congress has also increased funding for the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security from $2 billion for fiscal year (FY) 2020 to $2.9 billion for FY23, a 45 percent increase. Further growth is expected in FY24. The nation will reap the benefits of these cybersecurity investments for years to come.

The executive branch has made productive changes. The Office of the National Cyber Director (ONCD) — having reached full operating capacity — issued a comprehensive National Cyber Strategy and associated implementation plan as well as the first-ever National Cybersecurity Workforce and Education Strategy. CISA has continued to improve its technical support to other federal agencies, establish cyber performance goals, and develop plans, sharing, and response efforts through the Joint Cyber Defense Collaborative. The Securities and Exchange Commission issued new rules to increase corporate responsibility for cybersecurity. The National Security Council has coordinated responses to an ever-increasing number of international espionage and malicious cyber incidents, while the National Security Agency has expanded and improved its information sharing and support efforts with targeted industry partners. Despite these efforts, federal agencies have an uneven record of collaboration with the private sector, although the Defense and Energy departments have made more progress than others.

Collaboration with the private sector is indispensable since deterring cyber threats depends on the resilience of the U.S. economy and the critical infrastructure that supports it, so the federal government cannot handle the job alone. Significant work remains necessary to build an effective cybersecurity partnership between the public and private sectors. This will require a careful balancing of incentivization, collaboration, and, only where necessary, regulation across and between each of the country's critical infrastructure sectors. A similar effort is needed to enhance cooperation with like-minded international allies and partners, ensuring a resilient global economy.

To support these efforts, the U.S. government must continue to empower existing cybersecurity agencies and invest in hardening its security posture. As part of this effort, the government should continue implementing the recommendations of the CSC. Congress created this commission to identify a strategic approach to securing cyberspace. Over the course of three years, the commission developed 116 recommendations, many of which are accompanied by model legislative language. Nearly 70 percent of these recommendations have been fully implemented or are nearing implementation, and an additional 20 percent are on track to be implemented.

This assessment details progress toward implementing the commission's original work, consisting of its report and white papers. The assessment also suggests actions that can be taken to accomplish more recommendations. We urge readers to consider this report as a way to gauge America's collective efforts, allowing many government and industry stakeholders to identify areas suitable for building or deepening partnerships to achieve the broader objective of protecting our national cybersecurity.

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

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

2023 Annual Report on Implementation

Jiwon Ma & RADM (Ret.) Mark Montgomery

Timeline

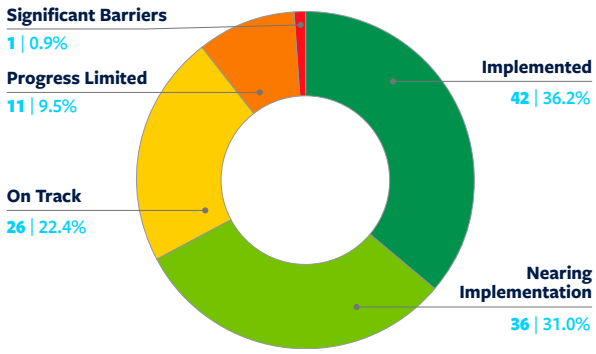
September 2022

- The Senate confirms Nathaniel Fick as the inaugural ambassador at large for cyberspace and digital policy at the State Department.
- The president issues an executive order expanding the factors considered by the Committee on Foreign Investment in the United States to include cybersecurity.

December 2022

- The Cyber National Mission Force becomes a subordinate unified command of U.S. Cyber Command, further reflecting its operational success.
- As part of the FY23 National Defense Authorization Act, Congress establishes the Bureau of Cyberspace and Digital Policy through the passage of the Cyber Diplomacy Act and authorizes the Federal Risk and Authorization Management Program to standardize security assessment of cloud computing products and services used for unclassified federal information.
- The FY23 omnibus spending bill authorizes over $2 billion in funding for CISA to carry out its responsibilities and $22 million for the Office of the National Cyber Director to fully staff its office.
- The Office of the National Cyber Director establishes the National Cyber Workforce Coordination Group, an interagency forum to address federal workforce and education challenges.

Progress Toward Implementation of All 116 Recommendations



March 2023

- The White House issues the National Cybersecurity Strategy, serving as the declaratory policy for U.S. cybersecurity policies.

April 2023

- Ambassador Fick announces that the Bureau of Cyberspace and Digital Policy is on track to place a cyber and digital officer in all U.S. embassies by the end of 2024.

May 2023

- The Department of Defense releases an unclassified summary of its cyber strategy.

July 2023

- The White House issues the National Cybersecurity Strategy Implementation Plan, a roadmap to execute the National Cybersecurity Strategy.
- The White House announces the U.S. Cyber Trust Mark program to create a voluntary cybersecurity labeling program for Internet of Things consumer devices.
- The U.S. Securities and Exchange Commission adopts rules for companies to disclose material cybersecurity incidents and cyber risk management practices to increase transparency and public awareness of systemic risks.
- The White House issues the National Cyber Workforce and Education Strategy.

August 2023

- The White House announces new initiatives aimed at bolstering cybersecurity in K-12 schools across America.