CSC 2.0

2025 Annual Report on Implementation

Jiwon Ma

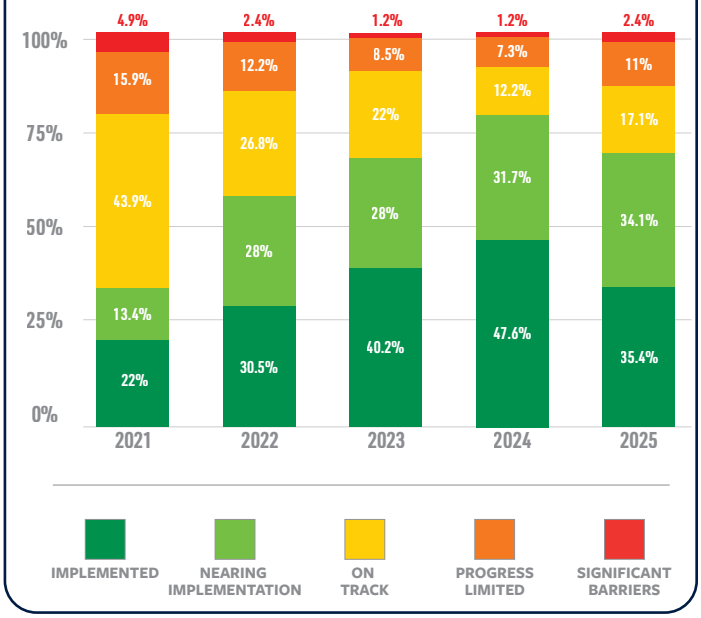
Executive Summary

Our nation's ability to protect itself and its allies from cyber threats is stalling and, in several areas, slipping. For five years, the U.S. Cyberspace Solarium Commission's (CSC's) recommendations have served as a benchmark against which to measure policymakers' commitment to strengthening the nation's cybersecurity. This report assesses that approximately 35 percent of the Commission's original 82 recommendations have been fully implemented, 34 percent are nearing implementation, and an additional 17 percent are on track to be implemented. By comparison, however, last year's report concluded that 48 percent had been implemented, 32 percent were nearing implementation, and an additional 12 percent were on track. For the first time, there has been a substantial reversal of the advances made in previous years. Nearly a quarter of fully implemented recommendations have lost that status — an unprecedented setback that underscores the fragility of progress.

Indeed, implementation alone does not guarantee institutional durability; key reforms remain vulnerable to underinvestment or bureaucratic gridlock that slows or prevents new initiatives from taking root. Personnel turnover and shifts in priorities during presidential transitions have historically also slowed cybersecurity progress. This year's assessment makes clear that technology is evolving faster than federal efforts to secure it. Meanwhile, cuts to cyber diplomacy and science programs and the absence of stable leadership at key agencies like the Cybersecurity and Infrastructure Agency (CISA), the State Department, and the Department of Commerce have further eroded momentum.

Implementation of any one set of recommendations is insufficient on its own to deter, thwart, or mitigate malign cyber activities. Rather, the Cyberspace Solarium Commission designed a new strategic approach — layered cyber deterrence — to reduce the likelihood and impact of significant cyberattacks.

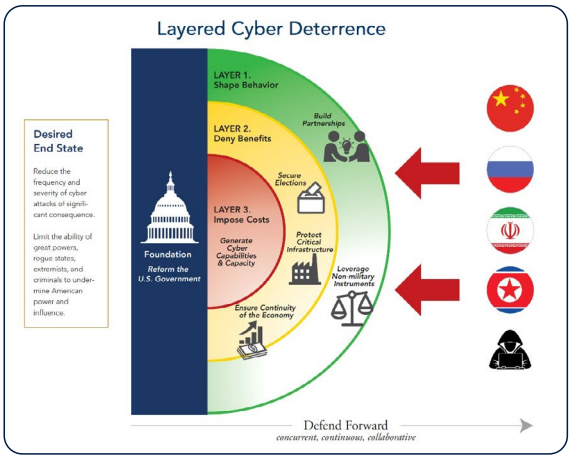
Progress Toward Implementation of the March 2020 Recommendations



Indeed, many of Washington's most important policy choices have reflected the Commission's strategy of layered cyber deterrence — the government has been shaping the behavior of foreign states while denying benefits and imposing costs on those who threaten democratic values in cyberspace. In some cases, this is directly through implementation of CSC recommendations; in others, it is indirectly through alignment with the CSC framework. Congressional and White House action have strengthened U.S. cyber resilience by expanding institutional capacity, improving interagency collaboration, and deepening public-private collaboration. But more work must be done.

Shaping behavior. The State Department's Bureau of Cyberspace and Digital Policy (CDP) plays a critical role in promoting responsible state behavior in international forums. Led by an ambassador-at-large, CDP is uniquely positioned to advance U.S. security and economic interests abroad, enabling federal agencies to focus on strengthening cyber resilience at home. The bureau needs a Senate-confirmed leader to be most effective.

Denying benefits. A successful whole-of-nation approach to deterring adversaries requires strong industry partnerships and stable Senate-confirmed leaders to carry out the mission. The Office of the National Cyber Director (ONCD) has driven strategic alignment across the federal enterprise, while the CISA has deepened engagement with critical infrastructure owners and operators and state, local, tribal, and territorial governments. Maintaining these partnerships has been challenging as contract lapses and the weakening of liability protections have strained trust. Private capital continues to reinforce these partnership efforts through initiatives such as Cyber Clinics that support both victims of cyberattacks as well as research and development programs that drive innovation.



Source: Cyberspace Solarium Commission

Imposing costs. U.S. law enforcement agencies and the Department of Defense (DoD) have reinforced deterrence by working with allies and partners to conduct persistent engagement and take down botnets before they reach U.S. networks. But attacks continue, indicating our adversaries are not being forced to bear sufficient costs for their malign activities.

What began as a forward-looking vision has become an urgent set of unfinished tasks. The challenge is to reinforce what has been built and address the gaps that remain. That requires a National Cyber Director with real budget and authority; empowering CISA and sector risk management agencies; restoring diplomatic tools and foreign assistance to extend U.S. reach abroad; and ensuring the cyber workforce can meet tomorrow's challenges. Building a more robust domestic response capacity is also becoming a clear need. Lastly, achieving these goals will require reestablishing bipartisan consensus on cybersecurity as a core element of national security.

The United States faces a pivotal decision point. It is up to the administration and Congress to seize this opportunity to secure the gains of the past five years; reinforce its cyber deterrence posture; and send a clear signal of capability, intent, and continuity to its adversaries.

Senator Angus King (advisory)
Former Chairman of the
Cyberspace Solarium Commission

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**