What You Need to Know About the Cybersecurity Solarium Commission Report

Deterrence, speed and a collective approach to defense are the core concepts of the new strategy.

James Mersol
Fri, 03/20/2020 - 14:54

The Cybersecurity Solarium Commission's recently released report outlines a strategy to fundamentally reshape the U.S.'s approach to cybersecurity and prepare for resiliency and response before a major cyber incident occurs, not after. Unlike the original Solarium Commission, which operated in a classified environment, the Cybersecurity Solarium Commission chose to release its report publicly out of recognition that cybersecurity involves everyone.
“In studying this issue,” begins the letter from Sen. Angus King and Rep. Mike Gallagher, the chairmen of the commission, “it is easy to descend into a morass of classification, acronyms, jargon, and obscure government organization charts. To avoid that, we tried something different: an unclassified report that we hope will be found readable by the very people who are affected by the very people who are affected by cyber insecurity – everyone. This report is also aimed squarely at action; it has numerous recommendations addressing organizational, policy, and technical issues, and we included an appendix with draft bills that Congress can rapidly act upon to put these ideas into practice and make America more secure.”

The commission’s report is simultaneously broad and detailed. A common theme running through it is that simply adding a new agency or reworking a few policies is insufficient to properly align the nation towards an effective cybersecurity strategy. The recommended strategy, which the report dubs “layered cyber deterrence,” is based upon “the need to reform how the U.S. government is organized to secure cyberspace and respond to attacks.”

That overarching goal and need rests upon three layers of deterrence, six pillars of policy and over 75 concrete recommendations that touch upon multiple federal agencies, Congress and the White House.

The three layers — shaping behavior, denial of benefits and cost imposition — call for a collective approach to cybersecurity, specifically urging the federal government to reach out to both the private sector and nation-state allies to shape norms, increase security and resiliency across the board, and identify and retaliate against adversaries.

The Cybersecurity Solarium Commission encourages the U.S. to pursue “deterrence by denial” by prioritizing resiliency across the public and private sectors, raising the costs on adversaries who seek to undermine critical infrastructure.

While government frequently looks to industry for innovation, the report stresses this partnership is necessary for both the public and private sector to pursue a whole-of-nation defense.
“Raising the baseline level of security across the cyber ecosystem — the people, processes, data, and technology that constitute and depend on cyberspace — will constrain and limit adversaries’ activities,” the report says. “Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes.”

During the commission’s process, it met with over 100 private-sector organizations, as well as 24 academic institutions.

Other key recommendations the report makes include establishing select committees on cybersecurity in both houses of Congress, heavily investing in the Cybersecurity and Infrastructure Security Agency (CISA) to give it the resources and authorities necessary to be the chief agency in charge of national cybersecurity and resiliency, and establishing and funding a “National Cybersecurity Certification and Labeling Authority” to manage security certifications, including cloud security certifications on a national level.

The commission also recommends establishing a National Cyber Director within the Executive Office of the President, a position that would serve as “the President’s principal advisor for cybersecurity-related issues, [and will] lead national-level coordination of cybersecurity strategy and policy, both within government and with the private sector.”

While there is already a federal CISO position within the Office of Management and Budget (OMB), the commission’s recommendation is designed to create a position with even greater authority over cybersecurity, working directly with the president as well as with both the public and private sectors.

The report is notable as one of the first government documents to recommend collective defense as a strategy, said one source. It is also rare for a commission to provide concrete action items, such as draft legislation and resourcing recommendations.

“Policy without resources is rhetoric,” said Frank Cilluffo, one of the commissioners, at the 2020 RSA Conference. “We recognized that and identified some areas where plus-ups are needed.”
“I rebelled initially at the recommendations for increased funding,” explained Suzanne Spaulding, another commissioner. “On earlier commissions that I’ve been involved with, there was sort of a general feeling that we weren’t going to make any recommendations for increased resources because that’s such a cop-out — it’s an easy thing to do, and it’s not going to happen. I got over it because in this area, countering malicious cyber activity, we are so dramatically under-resourced across the board.”

The Cybersecurity Solarium Commission adopted the Defense Department's strategy of “defend forward” for cyberspace, encouraging the federal government to use all tools at its disposal, but focus on reducing the number of attacks that seriously harm the U.S. but “do not rise to a level that would warrant the full spectrum of retaliatory responses, including military responses.”

“Defend forward posits that to disrupt and defeat ongoing adversary campaigns, the United States must proactively observe, pursue, and counter adversaries’ operations and impose costs short of armed conflict,” the report states.

Although realigning the nation’s strategy toward cybersecurity may be a herculean task, the Cybersecurity Solarium Commission intended its recommendations to be realistic and measurable. The executive summary asks that Congress “consider ways to monitor, assess, and report on the implementation of this report’s recommendations over the next two years.”

“[We] made the decision to not take a blue-sky, aspirational approach that was not realistic,” said Spaulding, “but instead to focus on what is achievable.”

The chairmen’s letter on the report also emphasizes “speed and agility” throughout its discussion of layered cyber deterrence, calling for a proactive defense and quick response to any attack.
“We didn’t solve everything in this report,” the chairmen said. “We didn’t even agree on everything ... Yet every single Commissioner was willing to make compromises in the course of our work because we were all united by the recognition that the status quo is not getting the job done. The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility. We all want that to stop. So please do us, and your fellow Americans, a favor. Read this report and then demand that your government and the private sector act with speed and agility to secure our cyber future.”

View printer friendly version
Federal Cybersecurity
Cybersecurity Solarium Commission
Cybersecurity and Infrastructure Security Agency
federal CISO
deterrence
Congress
Standard