Strengthening CISA Can Secure Vaccine Research, Experts Say

Following major cyber incidents, cybersecurity experts push for CISA support and a National Cyber Director.

Kate Macri
Mon, 07/20/2020 - 18:04

Sen. Angus King speaks at National Library Legislative Day in Washington in May 2014. Photo Credit: ALA Washington Office / CC BY-NC 2.0
Less than 24 hours after the National Security Agency accused Russians of using cyberattacks on COVID-19 vaccine research centers and Twitter reported a major cyberattack, members of the Cyberspace Solarium Commission implored Congress to instate a National Cyber Director and strengthen the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) so the U.S. government and private sector can better prepare for, prevent and protect against cyber threats.

“[This is] just a reminder that this is not an academic question,” said Cyberspace Solarium Commission Co-Chair Sen. Angus King (I-Maine) at a House Committee on Homeland Security hearing Friday.

King said the U.S. government needs to invest in layered cyber deterrence — a key principle of the commission’s March report chock full of cybersecurity recommendations — and ensure there are consequences for nation-state hackers and cyber criminals.

“[Layered cyber deterrence] means resilience so that our adversaries feel there's not much to be gained by attacking us because of our security and protection of our systems, but also a declaratory policy that if attacked we will respond,” King said at the hearing. “One of our deficiencies in our cyber posture is we have a deterrent policy for a major threshold of force, but we haven't had a major strategy that would provide a deterrent for cyberattacks. For that reason, we're a cheap date. Our adversaries don't compute the cost of attacking us. That has to change.”

King criticized the government’s “messy” approach to cybersecurity policy, quipping that “messy structure equals messy policy.” A National Cyber Director, he argued, will ensure continuity and consistency in national cybersecurity policy.

“We want someone in the federal government who wakes up every morning with the mission of protecting this country in cyberspace,” he said.

Suzanne Spaulding, a commissioner for the Cyberspace Solarium Commission and former undersecretary for cybersecurity and infrastructure at DHS, recognizes that with more funding CISA can be an effective agency combating cyber threats.
“With malicious actors targeting hospitals, vaccine development and government at every level, CISA’s work has never been more important,” she said at the hearing. “This is why the commission urges Congress to provide CISA with the resources and authority including administrative subpoena authority. [CISA] needs to be the national risk manager to serve as the central civilian cybersecurity authority, to support local government and the private sector, identify systemically important critical infrastructure, and coordinate planning and readiness across government and the private sector.”

Spaulding also urged Congress to establish a national cybersecurity labeling authority, publish guidelines for secure cloud services, create a bureau of cyber statistics, help facilitate a “more effective and robust” cyber insurance market, and pass a national data breach notification law.

With the 2020 election fast approaching, she added, election security and cyber resilience is more important than ever.

“Paper ballots, for example, are a way of building resilience into our election infrastructure,” she said. “Replace outdated equipment, ensure voter verifiable paper-based systems and conduct election audits, these are perhaps the most urgent of our recommendations.”

Rep. Mike Gallagher (R-Wis.), co-chair of the Cyberspace Solarium Commission, also emphasized the need for a National Cyber Director and a stronger CISA, which he said could help solve what he calls the “human problem” of cybersecurity.

“Strengthening CISA is probably one of the most important recommendations in our report,” he said. “It's not just a matter of better enabling CISA or giving CISA the authority to do persistent threat hunting on .gov networks, it's also a matter of making the mission of CISA so appealing that CISA can compete for talent with the likes of Google, Apple, Facebook and win.”

CISA can’t compete with Silicon Valley on pay, he said, but can compete on mission if the agency has an “elevated” position within the government community.
“By giving CISA the elevated position, we believe we can solve the human element that is endemic to every cyber issue,” he said. “In the Twitter hack, they fooled a human being into giving credentials that facilitated an attack. Empowering CISA, giving the director a higher level of authority, is a step toward solving human problems in cyber.”

Rep. Kathleen Rice (D-N.Y.), praised the commission’s work and said “shame on us” if Congress didn’t fulfill every recommendation in the commission’s March report, which King described as a report intended to anticipate cyber catastrophe and brainstorm the best ways to prevent a major cyber incident from occurring.

“We wanted to be the 9/11 report without 9/11, and that’s what we wanted to focus on in this project,” King said. “The unthinkable can happen, but we can be prepared, we can prevent, and we can protect this country.”