Consistent Support Crucial for Election Security, CISA Director Says

Christopher Krebs advocates for a long-term, actionable plan to support state and local electoral commissions.

James Mersol

Thu, 09/19/2019 - 16:39

CISA Director Christopher Krebs speaks at GovernmentCIO Media & Research's Cybersecurity CXO Tech Forum on Oct. 4, 2018. Photo Credit: Geoff Livingston/GovernmentCIO Media & Research

Nearly every one of the 50 states is on the right path to “Protect 2020,” CISA Director Christopher Krebs said at the CISA Cybersecurity Summit Sept. 19, but developing a consistent, actionable plan in conversation with those governments will be essential for both the next election and the ones to come.

The $250 million that the Senate has allocated toward election security is a “good start,” Krebs said, but it is not “something they can set their budgets and watches by.” Instead of a one-time cash injection, Krebs encouraged federal cybersecurity leaders to engage with state and local officials to understand where their risk management priorities lie and what the cost of managing that risk will be.

“When I think about funding,” Krebs explained, “I think about three buckets.”

In his experience, state and local governments must first think about “the risk in the system now” — implementing paper ballot backups and removing direct recording electronic voting systems wherever possible. Online voting systems, too, are “too bleeding-edge for full-scale deployment,” he cautioned, instead recommending that federal and local agencies find a way to “strike a balance between security and voter participation.”

The second bucket focuses on a long-term “dependable stream of funding” for both hiring security professionals and issuing IT service contracts. In this role, the federal government can serve as a “dependable partner” not only for funding, but also for working with local governments to identify priorities in pursuit of an actionable plan.

“The Cyber Incident Response Plan is not an actionable plan in and of itself,” Krebs said. In its current form, it is a framework between CISA, the FBI and the Intelligence Community, but the next step is to tap into the experience and understanding on cybersecurity at all levels of the government to create “the implementing doctrine” to support the plan. States need to know what they can "clearly anticipate coming from the federal government,” Krebs said.

The third bucket is “an innovation fund” focused on utilizing the federal system as the laboratory for government cybersecurity just as it is a laboratory for democracy. It could take up to 10 years to get a nationwide cybersecurity process in place, Krebs said, and the innovation fund for states would help foster pilot programs and form the foundation of the long-term timeline to implement that process or even shorten the timeline.

Everyone is moving in the right direction for election security, Krebs underscored. Consistent funding and support nationwide will “give them a boost.”

View printer friendly version
election security

Christopher Krebs
Intelligence Community
Cybersecurity and Infrastructure Security Agency
Federal Cybersecurity
Standard