Rather than Chasing Threats, Homeland Security Dives into Risk

The first CyberCast episode explores how cyber relies on proper risk management.

Amanda Ziadeh

Sun, 07/29/2018 - 15:02

Illustration: iStock and Jon Halling/GovernmentCIO Media

Election infrastructure became officially recognized as a critical infrastructure subsector in 2017, and the Homeland Security Department has been working with federal, state and local partners to bolster information sharing and provide the resources needed to secure election systems and plan for response.

Election integrity is just one of the many topics Christopher Krebs, DHS undersecretary of the National Protection and Programs Directorate, talks about on the inaugural episode of CyberCast.

“I’ve spent a lot of time over the last year or so focused on the election security issue,” he tells podcast hosts Kiersten Todt and Roger Cressey. “The interesting thing about the way elections are run in the U.S. . . . it falls to the responsibility of state and local governments to administer and execute even national elections.”

That’s close to 10,000 election jurisdictions nationally, Krebs says. From a broader IT security perspective, state and local governments are not necessarily resourced on an annual basis for equipment refreshes, like upgrading licensing for operating systems or platforms. So, Krebs says DHS works to provide intelligence and information sharing, technical services, and instant response planning and exercises.

And part of the technical services is risk and vulnerability assessments.

“RVA is one of the topshelf offerings we provide,” Krebs says. It involves penetration testing and proper configuration evaluations in order to deploy the proper security footing. And what those RVA assessments are showing is basic cybersecurity hygiene needs; such as patching and updating, and appropriate administration of accounts and privilege limitations.

And in terms of information sharing and intelligence, Krebs says DHS is working to get the security clearances needed for state election officials. His division created the Election Infrastructure Information Sharing and Analysis Center, or the EI-ISAC, in February. In its first three months, the center reached participation from senior election officials in all 50 states.

Tune in to the weekly CyberCast to hear more about how DHS is preparing election security pilots that could scale in time for the 2020 elections. Plus, learn why focusing on contextualizing risk management, rather than chasing every cyberthreat is where DHS is pivoting its critical infrastructure security model.

View printer friendly version
Federal Cybersecurity
cyber
election
infrastructure
Department of Homeland Security
Christopher Krebs
CyberCast

critical infrastructure
National Protection and Programs Directorate