Front Lines
Agency battles epic disasters in 2018

BORDER PATROL
Immigration top priority

WOMEN IN CYBER
Combating gender gap

COOL CAREERS
Broad range of DHS jobs
Election Protection

DHS helps states secure voting

By Adam Stone

WITH THE SHADOW OF Russian meddling in the 2016 presidential vote still looming over the nation, U.S. Homeland Security Secretary Kirstjen Nielsen has put election security front and center of the department's priorities.

Threats against the election system are "real and evolving," she said in remarks this fall at the National Election Security Summit. She noted that in the past two years, "election security has emerged as one of the principal national security threats" facing the country.

DHS has been working closely with state authorities to tame that threat.

While election processes by law are the domain of state authorities, DHS in 2017 designated voting systems as part of the nation's critical infrastructure. As a result, there is much the department can do to help secure voting, said Matt Masterson, DHS senior cybersecurity adviser, National Protection and Programs Directorate.

Homeland Security gives state officials information about the evolving cyber land-

CONTINUED »

CYBER SPENDING

DHS has been partnering with private industry to secure elections and generally harden government systems against digital incursion for years. Recent contracts include:

- A $668 million award to ManTech to protect key government networks from cyberattacks.
- A $621 million contract with Booz Allen Hamilton for continuous diagnostics and mitigation of government networks.
- A $530 million award to CGI Federal to enhance the cybersecurity posture and risk awareness of federal government agencies.
At the Department of Homeland Security’s cybersecurity summit on July 31 in New York City, Secretary Kirstjen Nielsen stated that, “Cyberattacks now exceed the danger of physical attacks. ... This has forced us to rethink homeland security.”

scapes, specific threats and security best practices. The department also provides services such as “phishing campaigns,” in which spoof emails are sent to test government employees' ability to detect potential attacks, Masterson said.

At the request of state authorities, DHS will send experts on-site to work with state officials in a two-week risk and vulnerability assessment that includes testing vulnerabilities, evaluating architecture and creating mitigation reports. The department also can run remote scans on an election authority’s outward-facing networks and will produce a weekly report on vulnerabilities, Masterson said.

“DHS has a strong supporting role to play,” said Theresa Payton, CEO of Fortalice Solutions and former White House chief information officer. “They are there to provide threat intelligence, technical support and policy support. They can help with just-in-time actionable intelligence, lessons learned, suggestions for technical configurations.”

Masterson said DHS has some engagement around election issues with all 50 states, although the depth and breadth of that support can vary between jurisdictions.

“For each state, their needs are different, so each can choose what they need from us,” Masterson said. In addition to an election task force, DHS also makes field representatives, known as protective security advisers, available to tackle cyber issues. Regional directors also may offer resources. “On any given day, any one of those field folks may be in an elections office conducting an assessment or engaging with election officials.”

**PROTECTION PARADOX?**

Ironically, some worry that the success of these efforts could actually undermine election security. For example, former DHS undersecretary for cyber and infrastructure Suzanne Spaulding sees the department’s state-level efforts as a potential double-edged sword.

“We run a risk that people will be deterred from voting if the volume is turned up on the narrative that the system is rigged or cannot be trusted,” said Spaulding, now a senior adviser at the Center for Strategic and International Studies. “While it’s important to sound the alarm, we also don’t want to accomplish an adversary’s objective in undermining the system.”

Others say a big noise is just what is required. At the University of California Santa Barbara Center for Cybersecurity, professor Giovanni Vigna said DHS should go broader, looping academicians and researchers into its cyber efforts.

“As researchers, it’s our job to break stuff and put it back together. We have the expertise,” he said. “We should have as many eyes on this problem as possible because the election process is so unbelievably diverse. There is voter registration, vote collection, vote tallying, all carried out by different people. You have to consider all of that in your threat model.”

Given all the moving parts, DHS officials say voting won’t ever be 100 percent secure. The goal, rather, is to make voting “resilient,” Masterson said. “Our ability to detect incidents and to keep the process running — that’s what is critical.”