Critical Infrastructure… and Still Critically Underfunded: What Comes Next for Securing U.S. Elections?

By Kay Stimson

Without funding or resources to update outdated voting systems and software, states and localities are struggling to understand—and implement—the U.S. Department of Homeland Security's January 2017 designation of elections as "critical infrastructure." Many states support a push to have the Trump administration rescind the executive order. Election officials that oppose the measure are concerned about the lack of federal government parameters and the possibility it will create more problems at the polls than it solves, but national intelligence officials say it's necessary to properly secure the process against threats—particularly foreign-government cyberattacks. No matter what happens in Washington, state policymakers are asking: How can we protect and secure our voting process for the future?

State officials who oversee the voting process are calling for the Trump administration to rescind a new directive that assigns the federal government a broad role in securing state and local elections. Coming off a presidential election cycle marred by claims of election rigging and foreign interference, it's a fascinating twist in the national debate on how to secure the American voting process from threats and foreign manipulation. Most notably, it is not another battle across partisan lines.

"Secretaries of state who oversee elections are concerned about the establishment of unchecked executive power over our elections process, while our national security leaders view the need to secure voting systems from threats and attacks—particularly foreign cyberattacks—as justification for more federal oversight and involvement," said Indiana Secretary of State Connie Lawson.

Here's the backstory: In an eleventh hour response to election season hacking attempts by the Russian government, outgoing U.S. Homeland Secretary Jeh Johnson officially declared the electoral system as "critical infrastructure" on January 6, 2017.

Never mind that no credible evidence of hacking was ever discovered or presented when it comes to the casting or counting of ballots in the 2016 presidential election, as the U.S. intelligence community and several state-level recount attempts have verifiably confirmed.[1] Russian-led cyberattacks on political party email servers and phishing schemes against high-profile political operatives drove calls in Washington for a federal government response. Plus, two summertime incidents involving intrusions into online voter registration systems in Arizona and Illinois were linked to Russian sources, prompting the FBI to warn state election offices to increase their security measures for the November 2016 election.[2]

In an official statement, Johnson emphasized that the critical infrastructure designation did not constitute "a federal takeover, regulation, oversight or intrusion" for elections. The goal was to show the American public—and the world—that political meddling will not be tolerated and voting systems are hands off.

According to what the Department of Homeland Security, or DHS, had been able to learn in the run-up to Election Day, elements of the heavily decentralized U.S. election infrastructure were badly in need of fortification against future attacks by sophisticated foreign adversaries. Aging voting machines, a lack of resources for cyber security and murky legal questions about response to cyber incidents had concerned election verification advocates for years.

What few in Washington seemed to have anticipated, however, was that unilateral executive action to protect state and local election processes would set off its own set of cascading alarms.

Now the question is, what is the best pathway for securing elections? Is it developing greater uniformity and standardization, established with the help of the process set by the feds, or leveraging the diverse, decentralized system that has proven to be resilient against large-scale attacks for more than 200 years, but is badly under-resourced and in need of technological upgrades?

What Does it Mean to be "Critical Infrastructure?"

With preparations already underway for the next election cycle, state and local election officials are grappling with how the so-called "critical infrastructure" classification for elections will actually work. For starters, they want a better idea of what it will do to help them protect their online systems against hacking attempts.

"DHS says the designation provides a more institutionalized foundation for protecting our voting process from independent and state-sponsored attacks—particularly cyberattacks. Yet it comes with no added technical support, no funding to help upgrade systems and no additional help for states that do not wish to bring the federal government into their security process," noted Connecticut Secretary of the State Denise W. Merrill, serving as president of the National Association of Secretaries of State, or NASS, in remarks before the U.S. Election Assistance Commission, or EAC.[3]

Another challenge is ensuring that a hastily-formed subsector of critical infrastructure doesn't create more problems than it solves. According to DHS, the critical infrastructure designation was created in 2003 to cover "assets, systems and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[4]

In applying the designation to election systems, DHS grouped them under "government facilities," one of 16 existing sectors of critical infrastructure. The classification covers both cyber and physical elements of election systems, including "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[5]

In addition to providing technical support to secure election systems, DHS says other benefits include priority in federal government assistance and greater access to information on threats and vulnerabilities. Specifically, some election officials will be eligible for security clearances to get classified intelligence information.

These selling points have yet to sway most secretaries of state, who adopted a resolution opposing the designation in February 2017 at the annual NASS winter meeting.

"Designating the sixteen sectors as critical infrastructure hasn't actually protected them from hacking attempts," noted Georgia Secretary of State Brian Kemp, who as co-chair of the NASS Elections Committee has been an outspoken opponent of the federal government's decision. "Plus, elections are low-connectivity. Voting machines aren't supposed to be online or networked in any way. Internet-facing systems, like voter registration databases, don't impact official vote tallies."

While the federal government's help is currently described as voluntary, Kemp and others are wondering just how "voluntary" these commitments will be down the road. According to the Presidential Policy Directive (PPD-21) that guides the federal government's approach, DHS—not the states—becomes the center of work to protect the elections subsector. The feds must oversee a process of formulating a subsector risk profile with corresponding preparedness guidelines. There are myriad questions about whether this leads to additional oversight and regulation, possibly raising constitutional issues.

"I have yet to hear of a single secretary of state from either side of the aisle who is in favor of this designation," said Louisiana Secretary of State Tom Schedler. "When it comes to election integrity, I am not going to let the federal government have the keys to our secured election system unless they can better articulate their intentions."

Additional concerns exist regarding transparency. The Patriot Act affords all sectors of critical infrastructure with broad exemptions from public records and sunshine laws. How will classified briefings and confidential threat-sharing affect trust and confidence in our electoral process? U.S. government military and intelligence agencies can classify their work to shield it from public scrutiny, but this level of secrecy has never been applied to our elections.

"Right now, our system is designed to foster transparency and participation from end to end, from public testing of voting equipment to poll watchers to public counting of the ballots to post-election audits," added Merrill. "If the critical infrastructure designation reduces diversity, autonomy and transparency in state and local election systems, the potential of adverse effects from perceived or real cyberattacks will likely be much greater and not the other way around."

Most notably, who is going to pay the bills? Within the elections community, there is strong sentiment that funding and resources would be best focused on updating outdated voting technologies and supporting states and localities in protecting their own systems. DHS has already acknowledged the critical infrastructure designation doesn't come with any money for this purpose. The last round of significant investment in elections occurred through the Help America Vote Act of 2002, when the federal government provided a one-time infusion of roughly $3.65 billion dollars to states and localities for election modernization.

"Funding the next generation of election systems should be our greatest priority," said California Secretary of State Alex Padilla, who is seeking support for replacing voting systems that are approaching their useful end of life.

Padilla and others are concerned by the reality that despite the threats that were evident in 2016, state and local governments still tend to rely on outdated systems due to a lack of funding and technical support. A recent report prepared for California legislators references one county that is still using a voting system from the 1990s with computers running on Microsoft Windows XP. [6]

What can be Done to Protect State and Local Elections?

Wrangling over the election security landscape is unlikely to be resolved anytime soon, although DHS plans to have the new critical infrastructure subsector for elections set up in time for the 2018 election cycle. That means there is little time for dealing with limiting factors such as funding.

From registration to voting machines and paper audit trails, election officials throughout the U.S. are making plans to tighten up security. Critical infrastructure or not, the attention from Russia's reported attempts to wield influence in the 2016 election cycle has had a meaningful impact on state and local cybersecurity practices for elections.

"State legislators interested in this issue would be well-served by reaching out to their election officials about what is being done at the state and local levels to secure components of the election system, including online or electronic systems they use," advised Schedler.

Possible questions for election officials include:

- What processes and fail-safes are in place to provide security and integrity to the process?
- How do officials verify the accuracy and integrity of voting results?
- How do states and localities test their systems? How can the public witness these steps?
- What's the plan, in case something happens? What cyber hygiene protocols do states/local follow?
- What can be done to help upgrade systems and unsupported software? Are there additional risks or threats that require action?
- What are ongoing concerns about the federal government's critical infrastructure designation for elections?

David Wagner, a member of the EAC's technical guidelines committee establishing federal testing and certification standards for voting equipment, said, "the number one most important thing we can do for cybersecurity is make sure the systems are auditable."

While acknowledging that election auditing won't prove there was no hacking, Wagner believes it can ensure that outcomes are correct and no patterns of voting irregularities exist.

Groups such as Verified Voting have lobbied for audits and back-up paper ballots in all 50 states, warning that voting machines which rely solely on digital components may be susceptible to tampering and manipulation. While most states already offer such fail-safes, some states and many lesser funded counties still lack a voter verifiable paper trail.

Election officials seem to agree that the general trend will be going from a reactive posture to a more proactive one in securing and verifying the election process.

"We know there will be progress compared to where we were in 2016," added Lawson, "but we must also expect increasingly more sophisticated threats as well."

Notes

[1] See National Association of Secretaries of State (NASS), "Key Facts & Findings on Cybersecurity and Foreign Targeting of the 2016 Elections," March 20, 2017.

[2] Federal Bureau of Investigation Flash Alert, "Targeting Activity Against State Board of Election Systems," August 18, 2016.

[3] Testimony before U.S. Election Assistance Commission (EAC) Public Hearing on Critical Infrastructure Designation. April 4, 2017.

[4] *https://www.dhs.gov/critical-infrastructure-sectors*

[5] Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems, U.S. Department of Homeland Security. September 16, 2016.

[6] Taylor, Mac. "The 2017–2018 Budget: Considering the State's Role in Elections." California Legislative Analyst's Office. March 30, 2017.

About the Author

Kay Stimson is director of communications and special projects for the National Association of Secretaries of State in Washington, D.C. A former television news reporter who covered the state legislatures in Maryland and South Carolina, she often focuses on writing about state and federal policy issues for lawmakers.