United States House of Representatives — Committee on Homeland Security
Defending Our Democracy: Building Partnerships to Protect America's Elections
California Secretary of State Alex Padilla
February 12, 2019

TESTIMONY

Good morning and thank you Chairman Thompson, ranking member Rogers, and members of the committee for the opportunity to be before you today.

And thank you for convening this hearing to discuss our nation's election security readiness. For me, and for my colleagues in state and local government, this conversation could not be any more urgent.

The defense of our nation's election systems and infrastructure must be a top priority for all of government — federal, state, and local. After all, our democracy is under attack.

Elections officials throughout the nation have taken seriously the warnings we have received from federal intelligence agencies — that our elections have been and will continue to be a target for bad actors, foreign and domestic, who seek to disrupt our democratic process and undermine public confidence in our elections.

Elections officials know these threats to be true, because we see them every day. For example, in California, our internet-facing systems are pinged or scanned constantly. This activity is the equivalent of someone walking through a neighborhood, checking doorknobs, looking for unlocked doors. While these are not hacks or breaches, those conducting this unauthorized activity certainly have intentions.

If we agree that the integrity of our elections is a matter of national security, then we must act accordingly and recognize that elections officials are on the front lines. We are the first responders to attacks on our democracy.

Yet despite consistent warnings and evidence, our national response is severely lacking.

Most critically, we must rethink how we fund and administer elections.

In my testimony today, I will discuss what the federal government can do to further support states and local jurisdictions, and I will share what we are doing in California to better secure our elections.

I want to start by saying that DHS Director Chris Krebs and DHS Senior Advisor Matt Masterson have become tremendously valuable partners. They have demonstrated their commitment to quality and timely communication and coordination with state and local elections officials when issues or concerns arise.

When potential threat information has surfaced, they have reached out to us. When we read or hear of new threats, they are there to inform us of potential exposure.

The importance of this partnership underscores the danger of unnecessary government shutdowns. During the recent shutdown, Secretaries across the nation were notified that email responses and phone contact with DHS personnel would be suspended or delayed. As the 2020 election cycle is already ramping up, we cannot afford to lose critical contact with our federal partners.

Partnership with DHS and other national security agencies is only one necessary component of a comprehensive defense strategy.

Let's be honest, elections are underfunded and are too often a low priority for federal, state, and local governments. The last time Congress approved new funding for elections was through the Help America Vote Act (HAVA), 17 years ago, in the wake of the 2000 presidential election. And the investments made as a result of HAVA were by and large in equipment and technology that is now 20 years old.

Members of the committee, you would not settle for 20-year old technology and reliability on your cell phones; our voting systems should be no different.

The lack of sustained investment has resulted in outdated election infrastructure and understaffed elections offices. Across the country there are many elections officials in counties with small populations — and therefore small budgets — that don't even have their own IT staff.

In addition to being outdated, voting equipment in many jurisdictions is at or beyond life expectancy. As we meet here today, there are some elections officials searching on eBay for replacement parts for systems that are no longer supported by manufacturers. Others are utilizing operating systems that are so old, their vendor no longer provides tech support — meaning some voting machines cannot be patched or updated with the latest security software.

Simply put, too many elections officials are ill equipped to defend against 21st century threats.

We often say that our budgets are a reflection of our values.

If we genuinely value our democracy, then we must commit consistent federal support for election security and administration.

Members of the committee, respectfully, last year's appropriation of $380 million in cybersecurity grants to states was not new money, and it certainly was not enough. The $380 million was simply the final appropriation of HAVA funds. That was the last of the butterfly ballot and hanging chad money. That was not 2016, 2018, or 2020 cyber threat funding.

In addition to funding, Congress also has a tremendous opportunity to make the proven best practices for election security the national standard.

Among them:

- Rigorous testing and certification of voting systems with up to date security standards
- Requiring testing of voting systems for logic and accuracy before every election
- Paper ballots and a voter verified paper trail, for auditing, recount, and manual tally purposes
- Keeping elections infrastructure offline
- Post-election audits after every election

I suggest to you that this is the proven framework for better securing our elections as well as improving voter confidence. Deficiencies in our election security infrastructure can jeopardize public confidence in our democracy. If voters begin to think that their vote may not be counted, or may not be counted as cast, and they decide to not participate in an election as a result of that doubt, that is a form of voter suppression.

These are just some of the best practices that have served California well since long before the 2016 election.

And in response to the 2016 election, we doubled down on our efforts.

We established intergovernmental partnerships with the U. S. Department of Homeland Security, the Federal Bureau of Investigation, the Elections Assistance Commission, the California Department of Technology, the California Office of Emergency Services, the California Highway Patrol and county governments to ensure coordinated responses to cyber threats and incidents.

My office has engaged local elections officials in cybersecurity trainings, table top exercises, and information sharing. And I personally visited fusion centers in all regions of California to better position ourselves to coordinate in the event of a threat or incident.

We upgraded our technology infrastructure and established both an Office of Election Cybersecurity and an Office of Enterprise Risk Management within our agency.

Another lesson I've taken to heart is that your technology is only as strong as the staff that uses it. Cyber security tools are just that, tools — tools for our staff to utilize. This is why we have invested in specialized staff dedicated to cybersecurity and trainings for elections staff at the state level and with our local partners.

As part of our strategies in the new Office of Election Cybersecurity, last fall we launched "VoteSure," a first of its kind in the nation public education campaign to increase voter awareness about election misinformation online and to promote official, trusted election resources. The campaign included the launch of a new web portal with a variety of tools and resources for voters including the ability to verify registration status before going to vote, reliable polling place look up tools, and a dedicated email address for voters to report suspected misinformation. And in a first-in-state history effort, we emailed official election information and resources directly to voters.

In the days leading up to the 2018 General Election, our staff identified nearly 300 Facebook posts and Tweets with inaccurate and misleading information about the voting process. We reported them to their respective social media companies for review. 98% of the posts and tweets we reported were promptly removed by their respective platforms for not meeting their standards.

Our office also piloted a new voter status email alert program in seven counties—Madera, Napa, Orange, Sacramento, San Mateo, San Bernardino and Solano—for the 2018 General Election.

This new system automatically notifies voters whenever we have received a new registration or update to their registration record through our online voter registration website or a paper voter registration form. We plan to expand the program statewide ahead of the 2020 elections.

California's share of last year's HAVA appropriation was $34 million. Funds in the current year's budget is helping counties with costs of upgrading security of their connection to our statewide centralized voter registration database, known as VoteCal, and polling place accessibility.

At the state level, we are using a portion of the funds for:

- Support of county efforts associated with cyber security risks and infrastructure needs related to the statewide voter registration system, including important activities such as security assessments, penetration testing, and staff training.
- Support for county improvement of polling place accessibility and administration of elections.
- Support for county vote center implementation, which includes costs associated with new voting technology like ballot on demand, electronic pollbooks, remote accessible vote by mail systems and voting systems.
- Enhancements to VoteCal statewide voter registration system.
- Development of security training curriculum and training of counties.
- Support and guidance for counties implementing risk limiting audits.

By all accounts, 2018 was a success. In California, voters responded with record high voter registration and the highest voter turnout in a midterm election since 1982. And the election went as smooth as we could have hoped for.

But, the threats to our elections are ever evolving. And those who seek to undermine our democracy will increase their efforts both in frequency and sophistication.

My colleague, Minnesota Secretary of State Steve Simon, puts it best, "Election cybersecurity is like running a race without a finish line." It's not enough to keep up with nefarious actors who seek to undermine our democracy, we need to stay ahead.

To do that, we must constantly be learning, scrutinizing, testing, and upgrading our security — and that requires federal, state, and local entities to keep working together and to make the necessary investments.

Thank you again for your work to address these issues head on. I appreciate your leadership and look forward to answering your questions.