



Election Security Advisory

January 7, 2020

Update for Local Election Officials on Recent Activity and Preparations for 2020 Elections

Increased Threat of Geopolitical Tensions:

In just the first week of 2020, two significant events displayed not only the improvement in information sharing among election stakeholders but the resilience of systems and processes which we have installed.

In the first event, coordination between the West Virginia Secretary of State Office (WVSOS) technology team and teams from at least two other secretaries of state offices identified unusual activity from a foreign IP address that appeared to target election-related systems. Utilizing expertise from each of these organizations, including a West Virginia National Guard asset embedded within the WVSOS office, key information was discovered, compiled and reported to the Department of Homeland Security (DHS) and the Election Infrastructure-Information Sharing Analysis Center (EI-ISAC). Within 24 hours of that reporting, the EI-ISAC sent a warning to all states about the potential of nefarious action from that IP address along with recommendations for detection of and protection against such efforts.

The second event was the removal by force of the Iranian general, Qassem Soleimani. The very next day, DHS's Cybersecurity and Infrastructure Security Agency (CISA) held a briefing by phone with critical infrastructure stakeholders across the nation about potential retaliatory cyber strikes against U.S. assets, again with situational awareness and protective measure recommendations.

In both the Soleimani warning and the foreign IP incidents, key information was shared nationwide within 24 hours of the event. One could contrast this coordination, analysis, and warning with where we were as a nation just three years ago. At that point, there was extreme distrust and almost no election cyber communication between the states and our federal government. Today, one readily sees governments from local to county to state to national working collaboratively as they should to protect America.

One should note the DHS "Soleimani warning" was not just to election officials, but to American businesses, NGOs, private citizens and others as well. While DHS did not identify any specific threat, the fact that the federal government was on top of the situation, was identifying potential threat vectors (that Iranian hackers may already be inside systems and to be watching for something to "be activated") and was talking openly to all facets of our society, shows remarkable progress toward threat deterrence and detection. Just as impressive was DHS's sincere interest in hearing from all potential stakeholders, not only about what they were seeing within their infrastructures but more importantly, about their concerns.

Meanwhile, West Virginia has taken the warnings from DHS, and its analysis of potential concern from the foreign IP situation, and coordinated with County Clerks throughout the state. Because West Virginia got out in front and started training county clerks two years ago and has done so now three years in a row, we have perhaps the best trained and prepared clerks in the United States. With the rapid response of our clerks, West Virginia was the first state to submit a proposal, and then use the funds Congress appropriated, for election security before the 2018 election. We're poised to do so again with the next Congressional appropriation in 2020. Not only does every ballot/vote in West Virginia have a best-practice voter-verified-paper trail, but more than 70% of voters in the state will also vote via the most modern, secure Express Vote System in 2020.

The world we live in today is one where asymmetric warfare is the norm, and cyber-attacks have become the weapon of choice for rogue regimes like Iran. Russia's meddling in the 2016 election exposed vulnerabilities in western democracies in general, including the U.S. in particular. As the cornerstone of democratic governments, elections have become "ground zero," and disinformation via social media has become a significant vector of attack. West Virginia's mantra of "protect, detect, and correct" has become the rallying cry of our nation's election community to thwart cyberattacks, and Soleimani's death pinpoints our state's preparations. The people of West Virginia should take pride in knowing our election techniques, tactics and procedures are setting the bar high for election protection and election integrity across our nation.

Election Security Background:

Following the 2016 presidential election, DHS named elections "critical infrastructure." Such designation heightens the significance of that sector in our society, giving it extra protection, attention, and financing to harden it against foreign interference. Elections joined 16 other sectors -- such as power grids, transportation systems, nuclear power plants, Wall Street, etc. -- as critical infrastructure.

West Virginia Secretary of State Mac Warner led the push to get all secretaries SECRET security clearances, an effort which led to success by early 2018. Currently, DHS sponsors three state-level

clearances and has recently offered additional clearances to one at the state level and one at the local level. At Warner's insistence that communication improves between the federal government and the states, DHS began holding classified briefings for secretaries at least twice a year. These security clearances and classified briefings were followed by closer coordination, more frequent communication, and training between federal, state, and academic entities. By 2019, information sharing centers, training cycles, and frequent classified video teleconferences became more regular and broke down the remaining walls between the various stakeholders. We are now standing together, united against foreign - and domestic - bad actors attempting to meddle in U.S. elections.

West Virginia laid additional groundwork in response to this new designation. Very early in the process, Secretary of State Mac Warner teamed up with Major General Jim Hoyer of the West Virginia National Guard and identified a National Guardsman with a TOP SECRET security clearance and considerable cyber capabilities. The Guardsman (*name withheld for security reasons*) was put to work under the supervision of WVSOS Information Technology Director Dave Tackett, with the sole purpose of protecting the West Virginia election process from cyberattack. It became a model for much of the rest of the nation.

West Virginia County Clerks also helped produce an Incident Response Plan (IRP), which is in distribution for the 2020 elections. This manual amounts to a "continuity of operations" plan for almost any incident that may arise: bomb threat, cyber-attack, natural disaster, power outage, active shooter, etc. As another example of how West Virginia is leading the way, this week, the state is sharing the IRP with election officials across the United States to, perhaps, save them time and effort in preparing their own.

The ideas and leadership that have come out of West Virginia over the last three years have put the state on the leading edge of election security in the U.S. Both Elections Director Brittany Westfall and General Counsel Deak Kersey were selected to serve in leadership positions with the National Association of State Election Directors (NASSED). Additionally, Secretary of State Mac Warner was selected to serve as Co-Chair of the National Association of Secretaries of State (NASS) Elections Committee for the important upcoming 2020 election year. So far in this role, Warner has met with the former DHS Director Jeh Johnson to discuss his rationale for designating elections as Critical Infrastructure, as well as with FBI officials on the same issue.

At the National Association of Secretaries of State meeting later this month in Washington, D.C., Secretary Warner will brief all secretaries on why DHS named elections "Critical Infrastructure," and on the continuing cyber threats identified by the FBI from Russia, Iran, and other such bad actors. Warner is also currently serving on and was a founding member of the Election Infrastructure Subsector Government Coordinating Council, a group that sets the protocols for election critical infrastructure.

- End -