NASS
National Association of Secretaries of State

September 26, 2016

Open Letter from the Nation's Secretaries of State to Congress: Let's Work Together to Share the Facts about Cybersecurity and Our Elections

As Congress looks into national security concerns about cyber threats to our election, the nation's Secretaries of State who serve as chief state election officials are issuing this letter via the National Association of Secretaries of State (NASS). Our bipartisan message: States are on high alert and will continue to vigilantly monitor their election systems for ongoing cyber threats and vulnerabilities. Fortunately, we have an infrastructure in place that will enable election officials to deal with problems in both the short and long-run. Understanding some basic facts about our system is important.

Of course, with talk of "rigged" elections and Russian attacks, there is much cause for concern. Recent efforts to mine data from voter registration systems in at least two states serve as an important warning against international cyber threats. As our national security agencies work to address any attempts by nation-state adversaries to disrupt the presidential election and call its integrity into question, there are many questions to be asking, including what constitutes an appropriate response and how to prevent further intrusions.

As public officials at all levels of government collaborate on these issues, there are important ways in which we can work together:

1) **LET'S MAKE SURE THE AMERICAN PUBLIC UNDERSTANDS THE BUILT-IN SAFEGUARDS IN OUR PROCESS**

   Election officials are working overtime to help the public understand the components of our election process and some of the built-in safeguards that exist. Elections are largely administered by states and localities. Voting systems are spread out in a highly-decentralized structure covering more than 9,000 election jurisdictions and hundreds of thousands of polling locations. Machines are standalone and do NOT connect to the Internet. There are multiple layers of physical and technical security surrounding our systems. U.S. Department of Homeland Security (DHS) Secretary Jeh Johnson and FBI Director James Comey have both publicly stated that our process makes it highly unlikely that hackers can hijack election outcomes, as there is no central point of entry and NO NATIONAL SYSTEM to be attacked. In fact, there is no evidence that ballot manipulation has ever occurred in the U.S. via cyberattack.

   Election officials welcome questions about security, and there are a range of options for getting more involved in the process – including becoming a poll worker to witness the process first-hand!

2) **LET'S WORK TOGETHER TO KEEP OUR ELECTIONS SECURE**

   Just as we must have contingency plans for floods and all kinds of natural phenomena, we must also be ready to deal with man-made threats. The risks posed by foreign government hackers, cyber criminals and everyday hacktivists are not new to election officials. States and localities

are committed to working with national security agencies and other federal partners, including the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST), to solicit input on threats and risk mitigation in our elections. States are already deploying numerous resources for this election cycle, including extensive testing for cyber threats described by the recent FBI alert, and best practices guidelines produced by the EAC. Additional steps may be taken based upon credible or specific threats that are identified in the run-up to Election Day. Secretaries of State are also part of a DHS Election Infrastructure Cybersecurity Working Group, created for sharing resources, best practices and technical advice.

To be clear: The equipment that people vote on is NOT connected to the Internet. Vote counting is NEVER done with systems connected to the Internet, and tabulation systems are not networked. Election systems must be physically secured when not in use, with public accuracy and performance testing that anyone can observe. Post-election audits can help to further guard against deliberate manipulation of the election, as well as unintentional software, hardware or programming issues. Again, there are no documented cases of flawed voting results linked to alleged cyber hacking.

3) LET'S NOT CONFUSE NON-VOTING SYSTEMS WITH OUR VOTING SYSTEMS

Election management and voter registration systems make the voting process more efficient and accessible, but they are not linked to vote casting or counting. While it is theoretically possible to disrupt an election via networked systems, their compromise will not affect election results. These systems have their own fail-safes and contingency solutions that would make it highly difficult to leverage them for changing outcomes. Poll books, printed records, back-ups and back-ups of back-ups all provide multiple layers of security around this part of the process. Plus, information collected through online voter registration systems typically does not flow directly into statewide registration databases. Instead, voter information is sent to each local registrar of voters for processing.

Most importantly, anyone who discovers an issue with their voter registration status when they show up at a polling place will still have options for casting a ballot. Every state has routine procedures for assisting voters whose names don't appear on the voter rolls. Adding names to rolls won't help, unless hackers also have an army of impersonators on the ground to help perpetrate their scheme, and voter impersonation has been documented as a rare occurrence. Both DHS and FBI officials have declared these scenarios to be highly unlikely, instead pointing to "sowing doubt or confusion" as worst-case outcomes, which election officials would be able to address. Voters can also check their voter registration status through www.Canivote.org.

4) LET'S SUPPORT INVESTMENT IN OUR VOTING PROCESS

It is no secret that elections are underfunded and under-resourced. The bipartisan Presidential Commission on Election Administration (PCEA) identified an "impending crisis in voting technology" as a key issue to address in its final 2014 report. There is no quick fix for this reality.

For that, we need a longer-term investment in our elections at all levels of government. Many states and localities want to replace or update their aging voting equipment, which is approaching its useful end of life. These systems were purchased by federal funding from the Help America Vote Act (HAVA) in the years following the contentious presidential election in 2000. In 2010, NASS produced a funding report noting that $396 million in HAVA funding remains to be appropriated by Congress.

Let's explore how an investment in voting technology can benefit the security of our nation's election process for the long-term, including cyber security as it relates to the federal development of voluntary voting systems standards for testing and certification overseen by the U.S. EAC and NIST. Besides asking what the next generation of voting technology will look like and how it will be secured, we must also determine how it will be adequately funded. This includes any kind of training that will be necessary to prepare the mammoth force of dedicated election officials and volunteers who run our system.

5) LET'S NOT TAKE ANY ACTIONS THAT WOULD UNNECESSARILY DAMAGE PUBLIC CONFIDENCE IN OUR PROCESS

There is no single piece of legislation or simple bureaucratic solution that can address all of the complex cyber security issues facing election officials, political parties and campaigns. While NASS currently has no position on a critical infrastructure designation by DHS, it has been made clear by Secretary Johnson that it will not come with additional funding for states and localities, and details on how this designation would be applied to elections are unclear. Some of our members have raised questions about how it would be possible to maintain public confidence in our elections, which are built on transparency and public access, if they are intermingled with national security agencies that understandably depend upon secrecy in their function. Others have been vocal in their view that such a designation would undercut the constitutional role that states and localities play in our elections and complicate the ability of states to work together with federal partners to combat cyber threats.

In the short-term, our goal is to avoid distractions and work together with our federal partners to secure the systems that are in place for the November election. Long-term, a larger dialogue is needed to avoid actions that would interfere with – or simply be perceived as interfering with – public ownership of elections by local communities and the citizens who run them, or be seen as threatening transparency and trust in our imperfect, but time-tested system of participatory democracy. Our collective imperative must be to ensure that actions to protect our elections do not create undue alarm or mistrust that will threaten voters' confidence in the outcomes.

Be sure to talk to your state and local election officials if you have additional questions. As we head into high gear for Election Day, Secretaries of State are taking every precaution to deliver a voting process that is not only safe and secure, but also fair, accurate and accessible. Voters must have no doubt that their votes – and votes alone – will determine the next President of the United States this November.