

Testimony of Michael Haas
Administrator
Wisconsin Elections Commission

United States Senate Select Committee on Intelligence
June 21, 2017

**Elections Security:
Lessons Learned and Continued Vigilance**

Chairman Burr, Ranking Committee Member Warner and Committee Members:

Thank you for the opportunity to provide information to the Senate Select Committee on Intelligence about what states learned from the 2016 elections and some steps that states are taking to secure elections systems as we prepare for future elections. I am honored to provide some thoughts on behalf of the National Association of State Election Directors (NASSED) and our President, Judd Choate, the state elections director of the State of Colorado, who is unable to be here today due to family commitments. I am a member of NASSED's Executive Board as its Midwest Region Representative.

Diversity of State Election Administration Systems

Before discussing the security of voter registration databases and voting equipment, it may be helpful to provide some brief background about the differences in election administration among the states, which is a true reflection of our federal system. In many states, the elected Secretary of State is designated as the state's chief election official, while the Lieutenant Governor serves that role in a handful of states. The state may have an elections director who is part of those offices and/or an elections board. Wisconsin has a unique structure with a bipartisan Elections Commission made up of three Republican appointees and three Democratic appointees, which oversees the agency and which appointed me as the agency's nonpartisan administrator and the state's chief election official.

At the state level, chief election officials and staffs are responsible for administering and enforcing election laws and procedures. This includes maintaining the statewide voter registration database as required by federal law, approving and sometimes purchasing voting equipment used in the state, training local election officials and poll workers, collecting and certifying official election results, and providing information to voters. In most states, elections are actually conducted by county clerks or registrars. Eight states, including Massachusetts and Michigan, conduct elections at the local level. In Wisconsin, we have 1,853 municipal clerks who conduct elections. As in other states, our agency is responsible for training each of those clerks so that election laws and voting procedures are administered properly and consistently throughout the state.

Finally, there are differences among the states in how voting and voter registration is conducted and in the ways that technology solutions are used. Some states maintain their voter registration database in-house and others rely on vendors. In recent years, states have developed and implemented various tools such as online voter registration, universal or automatic registration, electronic poll books, electronic transmission of blank ballots to absentee voters, and cross-state sharing of voter data in different combinations and on their own timetables. Some states use vote centers rather than traditional neighborhood polling places. Three states – Oregon, Washington and Colorado – hold elections entirely by mail.

These variations among the states illustrate different approaches but the same basic goals – to ensure the right to vote of every qualified elector, ensure the security of election systems and processes, maintain current and accurate voter lists, accommodate evolving trends in voter behavior, and reduce opportunities for administrative or human error. Ultimately, the common goal of election officials is to obtain the most accurate count of the vote so that candidates, voters and the public will have the utmost confidence in the integrity of our elections.

Regardless of the particular structure and tools of election administration among the states, several basic lessons were reinforced in the 2016 elections, although sometimes in a new context.

Effective Communication

First is the importance of constant, timely and effective communication with all of our partners so that all actors in the system have the tools they need. For example, the Elections Assistance Commission (EAC) develops many guides and other resources for election officials. NASED and other organizations such as the Election Center and the Election Academy provide professional education, training and tools.

At the state level we must communicate effectively with both federal agencies and local election officials. A simple example of this was the U.S. Postal Service's change in mail delivery standards. Last year the Postal Service advised that voters mailing in an absentee ballot do so at least a week before Election Day, even though many state laws establish a later deadline for voters to request absentee ballots. State election officials needed to communicate this change in policy to voters and encouraged local clerks to do the same.

The new twist in 2016 was the importance of communications regarding the security of election systems and equipment, specifically with the Department of Homeland Security and with the entities which provide cybersecurity protection to our voter registration databases. More than 30 states accepted DHS's offers of assistance leading up to the Presidential Election, including cyber hygiene scans of voter registration systems and other election technology, and risk and vulnerability assessments and recommendations. This assistance supplemented steps taken by state election offices and their respective

state IT agencies to monitor activity related to these systems and regularly consult regarding the status of those systems as well as security measures being implemented. States also increased cooperative efforts with the FBI and U.S. Attorneys, as well as state-level emergency management agencies.

In recent years many state election agencies have spent significant time educating state chief information officers and their staffs regarding the interaction of election processes with state IT infrastructure. A similar effort has taken place with the Department of Homeland Security since its emergence as a key partner in elections administration last summer. I believe DHS would acknowledge that its understanding of election administration was somewhat rudimentary when it entered this area last summer. Through communicating with secretaries of state and state election directors, its expertise regarding elections and appreciation for our concerns has improved but more can be done in this regard.

DHS would also readily acknowledge that some of its state partners have expressed concerns about the timeliness and the details of its communications regarding election security and potential threats to state systems. The recent reports about attempted attacks on state voter registration systems, which occurred last fall, caught many states by surprise. There is, of course, a balance needed between sharing information with those who may be affected and can take steps to address vulnerabilities and the need to maintain the confidentiality of information that is either classified or may have important law enforcement or national security ramifications.

State election officials understand that ongoing tension and look forward to working with DHS and other federal officials to develop protocols and expectations for communicating that type of information going forward. For example, state election officials believe it is important that they be in the loop regarding contacts that DHS has with local election officials regarding security threats such as the spear-phishing attempts that were recently publicized. After all, those attacks threatened state databases by attempting to gain access through a vendor and local election officials. States need to be aware of this information to protect their systems and so that we can provide additional training and guidance to local election officials.

As part of the DHS designation of election systems as critical infrastructure, bodies such as Coordinating Councils and Information Sharing and Analysis Centers can help to facilitate those discussions and decisions. NASED agrees with DHS that those bodies should consist of a broad representation of stakeholders.

I have provided to the Committee a copy of a letter from NASED President Judd Choate to DHS expressing our strong interest in participating on those bodies, and in forming them as soon as possible. State election officials are already in the midst of planning for 2018 elections and a fully functioning Elections Coordinating Council is important to the success of those efforts.

I would also note that the EAC has requested that DHS designate it as the Co-Sector Specific Agency at the federal level to provide subject matter expertise, resources and assistance in coordinating communications with state and local election officials. While the NASED membership has not taken a formal vote regarding the designation of the EAC as the federal Co-Sector Specific Agency, the NASED Executive Board endorses that request of the EAC.

Securing Voter Registration Databases

In addition to the importance of effective communication with our partners, the 2016 elections reinforced the need for constantly enhancing the security of voter registration databases. As DHS and election officials have tried to clarify, hacking into a voter registration system has no effect on the counting of ballots or tabulating election results. Voter registration systems contain data regarding voters, candidates, ballot contests, and polling places. If not prevented, intrusions could result in unauthorized parties gaining access to that information.

IT experts will note that no system is 100 percent secure from hacking. However, there is much that state and local election officials can do to improve the security of voter data. The 2016 elections demonstrated that many of these steps are not complicated, and the good news is that states are working to implement steps that will help detect and prevent hacking attempts in the future. In addition to the cyber hygiene scans completed by DHS and state IT agencies, some of those steps include greater use of multi-factor authentication for users of our systems, installing updated firewalls, the use of whitelists to block individuals using unauthorized email addresses or domain names from accessing the system, and completely blocking access from any foreign IP address.

Recently, David Becker, Executive Director of the Center for Election Innovation and Research, posted a helpful blog which placed reports of election system hacking into their proper context and recommended several additional steps for states going forward. These include conducting an analysis of voter registration activity in the days leading up to an election and comparing it to activity prior to past elections. For instance, queries may be completed to detect when multiple absentee ballots are requested for the same address, or to give additional scrutiny to requests that absentee ballots be sent to addresses out of the state and out of the country. Such queries may be an additional tool to ensure that only qualified and registered electors are receiving ballots.

Finally, states continue to improve their voter list maintenance practices by implementing more accurate and current data matching processes, with partner agencies both from the same state and across states. After a decade of experience matching data of individuals contained in the voter registration system with records from motor vehicle agencies and death records, some states are revamping their voter registration systems and rethinking those data matching processes. Keeping the voter registration lists accurate and up-to-date is a basic but crucial exercise which leads to efficiencies throughout the election process and minimizes opportunities for the misuse of outdated voter records.

Many jurisdictions are also participating in cooperative data sharing efforts across state lines. Wisconsin is one of 22 states and the District of Columbia which are members of the Electronic Registration Information Center (ERIC), which conducts comparisons of voter records from member states to identify individuals who may be registered in more than one state, or who may have moved within or between member states. More than 30 states participate in the Interstate Voter Registration Crosscheck Program, which attempts to identify individuals who have either registered or voted in more than one state.

In both cases, election officials may take steps to confirm the change in the voter's status and update records accordingly. What we have learned is that a possible computer match is not necessarily the same thing as an actual match involving the same individual, and the eyes of trained local election officials are still required to weed out real matches from the false positive matches.

Securing Voting Equipment

The final lesson of 2016 I would like to address relates to voting equipment. It is no secret that some jurisdictions throughout the country face challenges in funding the purchase of voting equipment to replace aging equipment which operates with older technology. In some cases, replacement parts are difficult to locate and vendors are discontinuing maintenance of the equipment. This remains a significant challenge which will continue to receive the attention of state and local election officials.

While not new, claims persisted in 2016 that voting equipment could be easily hacked and results could be altered. In the past, such claims were ostensibly supported by videotaped demonstrations of individuals who had physical access to individual voting machines and who installed malware into the tabulating software which counts the ballots. This represented an unlikely scenario in the real world given the processes used to program, test and secure voting equipment and programming software.

More recently, some have asserted that voting equipment can be attacked with malicious software remotely, through the election management software that programs equipment to count individual contests on the ballot and that is installed on individual voting machines.

To be clear, there has not been any evidence that voting machines or election results have been altered in U.S. elections. Still, election administrators must exercise vigilance to assure that such theoretical attacks do not become a reality. In order to maintain public confidence in election results, we must also continue to educate the public about safeguards in the system which help to prevent unauthorized access to and altering of voting equipment. These safeguards include the following:

- The decentralized structure of American elections means that multiple types of voting equipment are used across the country and often within individual states.

The diversity of equipment used and elections conducted at the local level help to create obstacles to large scale, coordinated attacks on voting equipment.

- In most cases, voting equipment is not connected to the Internet and therefore it cannot be attacked through cyberspace. When voting results are transmitted electronically on Election Night, it is after the polls are closed, the results are still unofficial, and they are transmitted using a cellular network rather than over the Internet.
- Approximately three-quarters of ballots cast in American elections are paper ballots, and most ballots cast on touch screen equipment result in a paper trail that can be immediately verified by the voter as well as by election officials through a recount or audit of the voting equipment.
- States implement overlapping and redundant processes to monitor and test the performance of voting equipment. Many states rely on the federal testing and certification program of the EAC and/or conduct their own testing and approval process before equipment may be used in the state. Public tests of voting equipment are conducted prior to each election and equipment is physically secured when it is not in use in an election. Finally, many states conduct post-election audits of voting equipment to ensure that votes are counted accurately as required under state law. As a result, Election Day is not the only time that voting equipment and its technology is under scrutiny.

Conclusion

In summary, I would reiterate that the American election system is characterized by decentralization, multi-faceted partnerships among federal, state and local officials, and constant innovations in the use of technology, data and best practices. The potential for disrupting election processes and technology by foreign or domestic actors is a serious and increasing concern. That lesson was clear in 2016 and continues to be a reality.

I believe I can state with confidence, however, the view of state election directors. Continued cooperation among those in the elections profession and in law enforcement, along with continued vigilance and innovation, will ensure the integrity of our voting processes and election results. We look forward to working with our federal partners as we plan for a full calendar of elections in 2018.

Thank you for the opportunity to share my thoughts with you. I would be happy to answer any questions that Committee Members may have.