NCSL

National Conference of State Legislatures

LegisBrief

A QUICK LOOK INTO IMPORTANT ISSUES OF THE DAY

JULY 2018 | VOL. 26, NO. 27

Securing Voter Registration Systems

BY DYLAN LYNCH

While state election processes in the United States are well defended, malicious actors have already identified and tried to exploit one facet of those processes: voter registration. Since there is every reason to believe attacks will happen again, election security has become the topic "du jour" for state and federal legislators, election administrators, policy wonks and the media.

The concerns about voter registration systems often take a back seat to concerns surrounding voting itself. And yet voter registration is the foundation for voting.

Experiences in 2016 showed why it is important to protect voter registration systems. According to a declassified version of the U.S. Senate Select Committee on Intelligence report, at least 18 states had their voter registrations scanned for vulnerabilities. In six states the malicious actors were, at a minimum, in a position to alter or delete voter registration data, although no evidence exists that this took place.

The graphic below depicts a basic outline of how most statewide voter registration systems work. These databases hold millions of records of individual voters, and they constantly receive or update data from many sources. These sources may include:

- The Department of Motor Vehicles, where many voter registrations are now initiated due to the Voter Registration Act of 1993 (aka motor-voter). Also, the DMV database is often used to verify voter registration information, such as name, address, date of birth, state ID number, etc.
- State online voter registration websites
- Local and state election officials' computers
- Other state agencies involved in voter registration

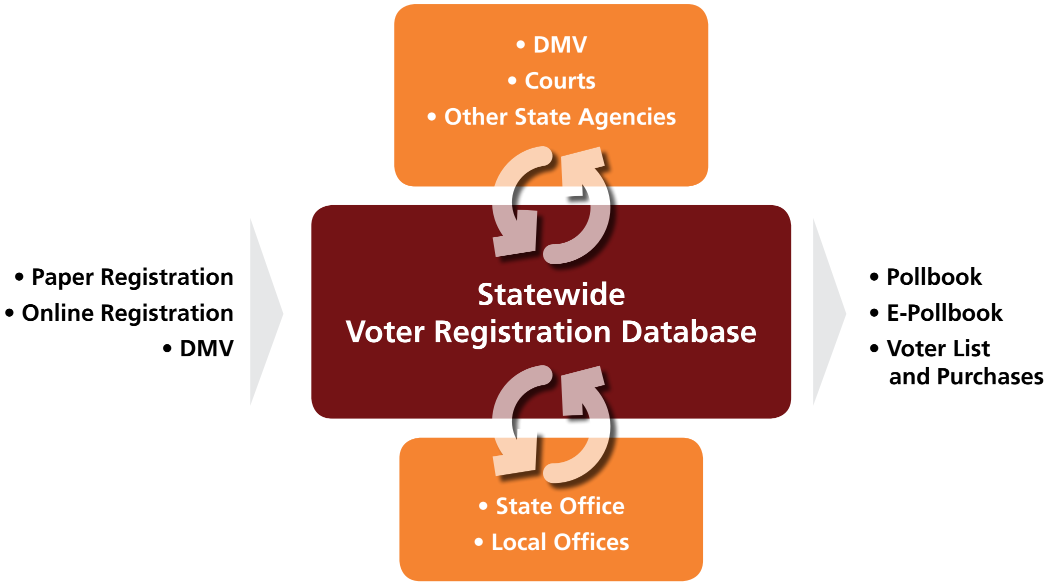
Did You Know?

• At least 18 state voter registration databases were scanned by Russian-affiliated cyber actors in 2016.

• The federal omnibus appropriations bill included $380 million for states and U.S. territories to improve their elections systems.

• Funding from the federal omnibus appropriations bill to upgrade election security will range from $3 million to $34.5 million per state.

Basic Outline of Voter Registration Sytem



If a voter registration system can be compared to a house, each point of contact (public portals, local election officials' computers, communication with other departments) is the equivalent of a door or window. A burglar trying to get into the house will try each point of entry and only needs one to be unlocked. Similarly, if cyber thieves find an "unlocked" point of contact, they potentially have access to all the data contained within the database and can do with it as they please. They could add, change or delete records, all of which would sow confusion, frustration and distrust. This kind of cyberattack could make Election Day chaotic and damage public confidence in the election system.

States—specifically legislators and chief election officials—can take many steps to reduce cyber risks to statewide voter registration systems. Some of these steps require legislative action; others may not.

■ **Upgrade or replace software and hardware.** Many states are running their registration systems on technology that is 10 years old or older.

■ **Back up data.** If malicious actors were to gain access and alter or delete registration information, how much data would be lost? Protocols to frequently back up data allow for easier recovery and correction if something goes wrong.

■ **Consider paper.** Many jurisdictions use electronic versions of voter registration lists, either on a tablet, laptop or desktop, to track and record voters at the polls. A simple fail-safe would be to have a paper copy on hand as well.

■ **Control access.** Who has and who needs access to the database? In local offices, does every temporary election worker need access to the system? Are there shared accounts? Limiting access to only those who need it may help reduce the number of doorways (vulnerabilities) into the system.

■ **Use two-factor authentication**. For those who are authorized to use the statewide voter registration database, cybersecurity experts suggest they sign in with two methods of personal verification.

■ **Audit logs.** Voter registration systems can create a log any time data is changed. Creating a baseline of activity and then periodically reviewing the logs against that baseline can help detect unusual activity that could be from a malicious source.

■ **Train staff on phishing/spear-phishing**. Phishing is an attempt to trick an individual to disclose personal information that may help a malicious actor gain access to a system. Often this includes links sent via email that may be opened by unsuspecting recipients. Training can teach election staff how to handle suspicious emails.

■ **Use CAPTCHA for online voter registration.** CAPTCHA requires a person to manually perform a task, such as clicking a box, typing in a word or selecting an image. This task is intended to stop computer programs (but not people) from engaging with a website, and could be used to secure online voter registration portals.

■ **Employ provisional ballots.** Provisional ballots are intended as a fail-safe method of voting for anyone who is eligible but not on the voter rolls for whatever reason. That reason could include a cybersecurity incident.

State Action

Legislators are turning concerns about cybersecurity and voter registration into policy. For instance, the Rhode Island legislature is considering a request from the secretary of state to use $1,550,000 of a $3 million grant from the federal government to upgrade the Ocean State's voter registration system.

In 2018, Maryland passed SB 281, which added the state administrator of elections or her designee to the Maryland Cybersecurity Council. Maryland also passed HB 1331, which requires the state elections administrator to report to the Department of Information Technology within seven days of becoming aware of a security violation (or significant attempt) of the election system. This includes the voter registration database and the online voter registration system.

Other proposed 2018 legislation includes California AB 2748, which would establish a pilot program requiring that an independent security assessment of the election infrastructure be conducted in participating counties. Illinois HB 4861 would appropriate money from the general fund to the state board of elections to be granted to counties for cybersecurity infrastructure. Ohio HB 466 proposes to establish a director of elections cybersecurity and an elections cybersecurity council.

Federal Action

In March 2018, Congress passed the federal omnibus appropriations bill, which included $380 million for states to improve their elections systems, including election technology and election security. States have until Sept. 30, 2023 to request their funds. States can use the money to upgrade election-related computer systems to address cyber vulnerabilities in voter registration or in other areas of the election system. The per-state funding ranges from $3 million to $34.5 million.

Additional Resources

- U.S. Election Assistance Commission, Common Cybersecurity Terminology
- The Belfer Center, Defending Digital Democracy, The State and Local Election Cybersecurity Playbook
- Center for Internet Security, A Handbook for Elections Infrastructure Security
- NCSL webpage, Election Security State Policies
- NCSL webpage, Voter Registration

NCSL Contact

Dylan Lynch
303-856-1532