Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 7, 2019

Election Security: Voter Registration System Policy Issues

Discussions about federal election security often focus on protecting voting machines and ensuring the integrity of election results, but voter registration processes may also be vulnerable to interference. Real or perceived threats to voter registration data could undermine public confidence in the electoral system. Altered voter registration data could potentially prevent eligible individuals from voting or allow ineligible individuals to vote in many states and territories. Voter data may also be a target for identity thieves or others seeking access to individuals' personal information.

For each state and territory (except North Dakota, which does not require voter registration), voter registration can be thought of as a system, organized around a centralized voter registration database (VRDB) containing individuals' names, addresses, and other information. The other components of a voter registration system can vary, depending upon state law and practices. Typically, a VRDB receives inputs from various sources (e.g., individual voters, local registrars, or other databases) to update its records. During an election, the VRDB is used to verify the eligibility of those who turn out to vote and is shared with local election administrators as *poll books* (or lists of eligible voters). Database information may also be shared with various sources for data verification, list maintenance purposes, or in the interest of public availability.

The VRDB and the ways in which it connects to other offices or entities involved in election administration (including vendors who provide software or equipment) can present security vulnerabilities. Some security vulnerabilities are related to cybersecurity or technology and others are related to human errors or actions. A state must generally ensure that its VRDB maintains (1) accurate records; (2) privacy for individual data; (3) accessibility for relevant actors; and (4) reliability during an election.

States have different policies regarding registration and the management of voter data, and some state or local practices may present bigger security challenges than others. Yet by having a variety of voter registration systems across states, potential problems that could arise may be limited to a few states or localities, rather than affecting a nationwide database or system.

Registration Security Issues in 2016

A July 2019 report from the Senate Select Committee on Intelligence (SSCI) on Russian interference in the 2016 election noted that VRDBs "were not as secure as they could have been," and detailed instances in at least seven states where voter registration systems were targeted for access, either directly or through connections between the central database and other governmental or election systems. In two of those states, the report found that VRDBs were inappropriately accessed. Although the committee found no evidence that registration data had been deleted or changed in 2016, its report notes that data obtained in the breaches may be held for use at a later date. The report also noted that the committee had "limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases."

Centralized State Databases

VRDBs may be targets for those seeking to interfere in elections or to access personal data on individuals. Each state with voter registration maintains a "centralized, interactive computerized statewide voter registration list," under Section 303 of the Help America Vote Act of 2002 (HAVA). According to the SSCI and other government reports, Illinois's VRDB was breached by cyber actors in 2016, resulting in exposure of voter registration data. These reports also note that another state's registration database may have been accessed in 2016 using a state employee's credentials obtained via email phishing.

Under HAVA, the required centralized VRDB must at least contain the name, registration information, and a unique identifier for every legally registered voter in each state. Other features of a state's database can vary, and it may include additional personal data about individuals. States also vary in their technical and administrative policies related to registration database management, such as the level of access granted to the database; what backup systems or audit trails are used; the degree of connectivity to other election systems or sources of registration-related data; and the process for removing inactive or ineligible voters from the database.

Sources for Updates or Verification

State VRDBs often receive or share data with other sources in order to verify new registrations, make changes to records, or to remove ineligible voters. Unauthorized actors may seek to access the VRDB or other election systems through these connections between the database and other sources. The SSCI report included three such examples from 2016. In one state, the committee noted that "at least one other government system connected to the voter registration system" was being scanned by outside actors. In another state, the committee found that the website for a district attorney's office had been targeted, possibly because its "most wanted" list "may have in some way been connected to the voter registration system." The committee also stated that multiple attempts were made to illegally access Vermont's online voter registration application, which was connected to the state's database.

In addition to the state election official(s) tasked with managing the database, a variety of other sources may transmit voter data to state election officials, including local election officials; individual applicants; government agencies offering registration opportunities (e.g., departments of motor vehicles [DMVs]) or maintaining vital records; or election officials in other states. Connections to various data sources, such as a DMV or the Social Security Administration (SSA) database, are commonly used to verify registration information received from applicants or to process registration status updates. Registration status changes can occur for a variety of reasons, often dependent upon state law, including changes related to an individual's name, residence, mental incapacitation, criminal status, or death.

States may also check registration information against other data sources for list maintenance efforts that seek to identify duplicate registrations associated with a single voter or to identify those who are ineligible to vote. The U.S. Postal Service's National Change of Address (NCOA) database, for example, is often used to identify voters who have moved outside of an election jurisdiction. States also might compare their registration records against other states' lists through partnerships or interstate organizations like the Electronic Registration Information Center (ERIC).

To preserve the integrity of the VRDB, states consider how information is added to, revised, or removed from its official records. States might allow connections between the VRDB and other sources to check information, but they can prevent any automatic changes from being made to registration records or prohibit data-sharing partners from viewing records in their entirety. Cybersecurity measures, such as firewalls or encryption, can help secure the networks or communications channels that connect a state's centralized database to other parts of a registration system. States can also engage in a variety of accountability measures related to the VRDB, such as establishing access control policies; limiting access privileges; requiring the consent of other officials for significant changes to the database; and utilizing an audit system to log any connection or change to the database.

Access to Registration Information

State election officials also share information from the VRDB for various purposes. Exporting information from the VRDB may also present security risks. States must typically have measures in place, for example, that prevent unauthorized changes to the underlying data from being made when it is exported from the database. States also attempt to provide appropriate protections to avoid disclosure of certain elements of registrants' personal information, such as Social Security numbers or driver's license numbers for purposes other than verifying that information with SSA or a DMV.

Voter registration information is often shared for list maintenance efforts. State voter registration information also usually must be shared with local election officials in order to administer an election. Local election administrators, for example, often need to prepare and deliver ballots to polling places in their jurisdiction based on the distribution of currently registered voters. On Election Day, poll books or lists of eligible voters are typically used at polling stations to verify the registration status for individuals who turn out to vote.

States generally also maintain a degree of public accessibility for voter registration data. Many states, and some localities, maintain websites that allow individuals to check their registration status at any time, which can be an important tool for catching errors that may have been recorded in the centralized database. States also typically allow entities or individuals meeting certain requirements to request access to, or purchase, a list of registered voters.

The data contained in a voter registration system can present identity theft or other personal privacy risks. For safety reasons, some states restrict disclosure of certain registrants' data, such as victims of domestic abuse or public officials. States can establish and publish privacy policies related to voter registration information that address limits on what personal data are collected; how data can be used and by whom; what security and legal safeguards are in place; and how access to specific records or data elements can be restricted under certain conditions.

Mitigating Election Day Effects

Maintaining the security of a voter registration system is an ongoing process for those who keep the database and its related components continually operating behind the scenes between elections. During an election, however, the accuracy and reliability of a database becomes particularly consequential. Errors related to individual records could prevent certain voters from casting ballots, or system-wide problems could affect all voters in a precinct or state. Any issue occurring on Election Day could undermine public confidence in the electoral process or outcome.

Voter registration deadlines, in some states, may prevent certain changes from being made to an individual's record immediately preceding, or during, an election. While such deadlines can provide an opportunity for election officials to verify information and secure their records, some deadlines may also inhibit a voter's ability to correct particular registration errors or altered data. States generally provide ways for voters to check their registration status, but reminders to voters to do so sufficiently ahead of an election or when list maintenance efforts occur may help prevent voters from learning of an issue only when they attempt to vote. Similarly, some states notify voters any time their registration information has changed.

If an issue with an individual's registration status arises at a polling place, the voter may cast a provisional ballot under HAVA. States, however, are often not equipped to use provisional ballots on a large scale, and vary in their processes for how final voter eligibility is determined and how such ballots are counted. To ensure election officials have accurate voter lists, jurisdictions also can maintain multiple means of accessing poll books, such as online access to the data, electronic data stored on an offline computer, and/or a printed paper list of registered voters.

Sarah J. Eckman, seckman@crs.loc.gov, 7-1834

IF11285