Voter Registration Database Security

A Research Report from the Center for Election Innovation & Research

By David Becker, Jacob Kipp, Jack R. Williams, and Jenny Lovell

September 2018
Who we are

The Center for Election Innovation and Research (CEIR) is a nonpartisan, nonprofit organization working to improve election administration through research, data, and technology. CEIR works with experts and election officials in every state and across the political spectrum to rebuild voter confidence in our elections and democracy, ensure all eligible voters can vote conveniently in a system with maximum integrity, and ultimately increase voter participation.

Authors

David Becker
Executive Director

Jack Williams
Research Associate

Jacob Kipp
Program Manager

Jenny Lovell
Research Associate

Thank you to Kesha Fitzhugh for her support on this project, and to Joseph Hall and Maurice Turner of the Center for Democracy & Technology for their contributions to the survey.

And thank you to the states that responded to the survey. The time and effort you put forth to thoughtfully answer our questions is greatly appreciated.

Media Contact

For any questions about this report, please contact us at media@electioninnovation.org, or reach out directly to Executive Director David Becker at dbecker@electioninnovation.org.
Executive Summary

The threat of foreign interference in U.S. elections is real. In the wake of the Russian government’s attempt to interfere with election infrastructure in 2016, states are taking cybersecurity more seriously now than ever before. Experts agree that attempts to interfere so far have been aimed at undermining Americans’ confidence in elections, not changing actual vote totals. That means attackers seem particularly interested in seeking to infiltrate systems like elections websites or voter registration databases, which are more readily accessible than the machines that actually tabulate votes. If those systems were compromised, it could create chaos and confusion that could further damage Americans’ faith in our electoral system.

In 2016, voter registration databases (VRDBs) were scanned in multiple states, though only one VRDB was successfully infiltrated. Since that time, the states have been making big improvements to their VRDB security in order to ensure they can entirely stop or quickly respond to any future attacks. To start a conversation about the current state of VRDB security, the Center for Election Innovation & Research (CEIR) convened a meeting in February 2018, which included over forty experts representing state and local election officials, technology experts, the Department of Homeland Security, the Election Assistance Commission, and others. CEIR subsequently conducted a survey of all the states, seeking to better understand the current state of VRDB security. The survey looked at three major areas of VRDB security: (1) prevention, (2) detection, and (3) mitigation. This report discusses the findings of that survey.

Based on the survey responses, it’s clear that states are taking securing their VRDBs seriously, though there’s still room for improvement. Significant majorities have implemented best practices for VRDB backups, cybersecurity training, and monitoring of VRDB access. However, states could still improve in certain areas. Many states, for example, need to review their password requirements and still need to implement multi-factor authentication.
**Introduction**

The threat of foreign interference in U.S. elections is real.¹ The Russian government attempted to interfere with election infrastructure in 2016, and those efforts will likely continue.² However, experts agree that the likely goal of that interference has not been to change actual votes, but to undermine Americans’ confidence in their own democratic institutions. Rather than targeting voting machines and vote counts, attackers mounted widespread misinformation campaigns³ and successfully infiltrated at least one state’s voter registration database (VRDB).⁴

Fortunately, despite attackers gaining access to a state’s VRDB, it appears no voter records were changed or deleted in 2016. But the possibility of tampering with the voter records exists. If an attack on a voter database was successful, provisional ballots could mitigate much of the risk to the actual vote-casting, but the chaos and confusion that would likely result from stressed poll workers, long lines, and frustrated voters could further damage Americans’ faith in our system.

---


5 52 U.S.C. § 21083(a).

6 North Dakota does not require its citizens to register to vote.

7 See, for example, the Center for Internet Security’s A Handbook for Elections Infrastructure Security. Center
information exists about the actual security measures currently in place. Thus, the Center for Election Innovation & Research (CEIR) has conducted a survey to assess the state of VRDB security in the United States.

The survey consisted of 23 multiple-choice questions addressing three major areas of cybersecurity: (1) prevention, (2) detection, and (3) mitigation. The survey was sent to election officials in all fifty states and the District of Columbia. Of those, twenty-six states returned completed surveys. Additionally, one state was able to contribute a small number of answers but declined to respond to most of the survey questions. That state’s answers are included in the analysis of the questions to which they responded. Three other states returned surveys which declined to answer any of the questions due to security considerations. Thus, those three states are disregarded in data-reporting and analysis.

This report details the results of the survey, while contextualizing the importance of certain security measures in maintaining a well-protected VRDB.

---


Regardless of its status as a state, commonwealth, or district, each survey respondent is anonymously referred to as a “state.”
VRDB Security in 2018
This report views the current state of VRDB security through a common three-pronged cybersecurity framework: prevention, detection, and mitigation. First, this report looks at how VRDBs are designed to prevent threats by controlling access, promoting system integrity, and training users. Next, threat detection through real-time monitoring and audits is addressed. Finally, state efforts to mitigate the impact of successful attack on their VRDBs are considered.

Prevention
The first logical step toward securing a VRDB is designing a system that is hardened to potential threats by eliminating as many security risks as possible. This includes controlling access to the VRDB, using secure tools and services, regularly auditing and maintaining the VRDB, and training users to appreciate and avoid the myriad of cyberthreats the VRDB could face. In this way, prevention is two-fold, consisting of both a digital side and a human side.

Access
Effectively controlling access is an important preventative measure for securing the centralized statewide VRDBs required under HAVA. In this context, “access” is used broadly, referring to both the ability to retrieve and manipulate data from a database. Although not all states’ VRDBs are designed the same way, every VRDB contains sensitive voter information. Additionally, many users need to have access to the database for a variety of reasons—to authorize address changes or confirm new registrations, for instance—and the number of users can vary significantly from state to state. Local and state election officials are the most frequent users, however, third parties (like technology vendors) may also need occasional access to VRDBs. Thus, it is imperative to properly manage user permissions as well as secure each instance in which a user gains access to the VRDB.

In every system, different users should have varying privileges that limit what they can view and change. Local election officials need access to voter records but usually not the underlying system infrastructure, whereas technology vendors may need the exact opposite. States seem to be doing very well in this area—100% of respondent states indicated that VRDB access privileges varied among different types of users.

Passwords
However, ensuring access security doesn’t end with good user privilege management. Another way to secure access to a VRDB is through the use of strong passwords and other authentication methods. Passwords may have varied requirements, such as how long they must be, how many characters they must contain, and how often they must be changed. States reported many different combinations of password requirements, such as a minimum length of eight to ten characters, a minimum of three different types of characters, and banning common passwords such as “password” or “12345.”
Most of the respondent states supported the use of strong passwords, using some combination of the above-mentioned requirements. Fifteen states also reported that they required users to change their passwords at least once every one to three months. Other states’ answers varied, some requiring password changes at least monthly, while four states never required password changes. However, it’s worth noting that requiring users to frequently change their passwords often leads them to reusing the same or only slightly different passwords.  

---

State Highlights: Colorado

In May, the Washington Post called Colorado the safest state to cast a vote, and Homeland Security Secretary Kirstjen Nielsen holds out Colorado as an example to other states. Our survey confirmed that Colorado is also among the best when it comes to securing its voter registration database. According to the survey, in addition to already using multi-factor authentication, backing up their VRDB daily, and monitoring their VRDB with an Albert sensor, Colorado places a premium on training its VRDB users. Users are trained at least once a year to understand cyberthreats, including the ominous threat of spear-phishing. In early September 2018, Colorado put its training chops on display with a large-scale table top exercise, which included election officials from throughout Colorado and across the nation. During the exercise, one scenario challenged participants by having the state voter registration database go down. Practicing real world situations like these and helping local election officials understand how to address them are one of the many reasons why Colorado is leading the nation in election security.

---

9 Five states indicated that they did not use any of the password requirements included in the survey. However, it is possible that they have some other requirement in place that was not reflected in the available survey answers.

Multi-factor Authentication
Multi-factor authentication (MFA) goes hand-in-hand with password security, and is a necessity for ensuring only authorized users are gaining access to a system. In order to verify a user’s identity, MFA typically requires the use of a password and a secondary authentication factor, whether that factor be physical, digital, or biometric. By requiring a second authentication step beyond a password, MFA can help combat common threats like phishing, which relies on users turning over their login credentials to would-be intruders. Half of the states responding have already employed MFA on their VRDBs, with at least one other state indicating that MFA is coming soon. Of those states already using MFA, physical devices were the most common secondary factor, being used by seven states. Three states reported using SMS verification and the two remaining states used time-based one-time passwords (TOTP) as secondary factors to verify login attempts.

Use of Multi-Factor Authentication

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>

- Physical (e.g., YubiKey)
- TOTP
- SMS
- Physical, SMS, and TOTP
- Not Used

System Integrity
Beyond securing access, VRDB systems should also have measures in place to maintain system integrity and prevent cyberattacks on an ongoing basis. In order to do that, systems need to be designed to make up for users’ security shortcomings. Though no one measure can ensure a system is secure, the combination of various security measures, knowledgeable system administrators and IT staff, and regular system maintenance can go a long way toward hardening a system against the threat of outside attack.

HTTPS
An easy way for states to promote system security is by using HTTPS for their websites, which encrypts information communicated between users and those sites. All responding states indicated that they use HTTPS on any sites that contain personally identifiable information. Additionally, of those states, twenty-two reported using HTTPS for all of their websites, regardless of content.

CDNs & DDoS Mitigation
While HTTPS can mask data in transit and prevent snooping, it is only part of a comprehensive security solution. Distributed denial-of-service (DDoS) attacks are a

---


common way for malicious actors to disrupt legitimate users’ access to a website or another networked computer system.\textsuperscript{13} Content distribution networks (CDNs) and DDoS mitigation tools are valuable ways to address the effects of DDoS attacks. CDNs redundantly maintain content over several servers—useful in case DDoS attack traffic is targeted at a single server or if a server is otherwise compromised.\textsuperscript{14} Dedicated DDoS mitigation tools, however, often are more focused in their approach. Typically, DDoS mitigation tools will first analyze traffic to establish a baseline, and then will redirect abnormal traffic before it reaches its destination.\textsuperscript{15} In practice, both CDNs and DDoS mitigation tools can be effective ways to ensure networked systems remain online and usable. More than a quarter of surveyed states said they use CDNs. Even more states—greater than half of the respondents—indicated that they use DDoS mitigation tools.\textsuperscript{16}

\begin{itemize}
\item \textbf{13} DDoS attacks work by leveraging various sources of traffic to overwhelm the bandwidth or resources of a target. See generally, Dhruba Bhattacharyya and Jugal Kumar Kalita. \textit{DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance}. Boca Raton: Chapman & Hall/CRC, 2015.
\item \textbf{16} Among states that reported using CDNs and DDoS mitigation, nine reported only using DDoS mitigation tools, two reported only using CDNs, and five reported using both.
\end{itemize}
Audits, security monitoring, and other VRDB system administration and maintenance tasks are typically handled by knowledgeable IT support staff. Every responding state had at least some IT support. The vast majority, twenty-one states, had a full-time IT staff member on their team. Four others reported contracting out to a third-party for full-time IT assistance. Only one state reported contracting out for part-time assistance.

Source of IT Support

- **Full-time Staff**: 21
- **Full-time Contractor**: 4
- **Part-time Contractor**: 1
- **Every Month**: 7
- **Every 1-3 Months**: 3
- **Every 3-6 Months**: 2
- **Every 6-12 Months**: 14

### IT Support

Just as a system needs to be designed to prevent as much human error as possible, so too must users be trained to minimize vulnerabilities. Even the most secure system can be compromised if a user decides to share credentials or engage in other risky practices. One of the most pressing problems in security today is the prevalence of phishing, which can trick even the most careful users into handing over their login credentials. That’s why it’s incredibly important that VRDB users are trained to be on the lookout for cyberthreats they might encounter.

### Phishing

Phishing and spear-phishing are common cyberthreats that target the human side of VRDB security by luring people in with fraudulent emails and tricking them into divulging personal information. In the 2016 presidential election, an alleged Russian influence campaign used phishing to gain access to sensitive documents and conversations. The states are well-aware of the dangers of phishing and are working to ensure VRDB users are, too. The vast majority of responding states indicated that

---


they trained all VRDB users about the threat of phishing and spear-phishing.¹⁹

Who is trained about phishing?

- All Users
- Some Users
- No Users

Email Security

Email protections, though not explicitly part of a VRDB system or security training, also go a long way toward preventing phishing attempts from succeeding. These protections usually work by verifying an email's sender or by checking the contents of a message. According to the survey, almost every state reported at least using spam filters, many in combination with other email protections like URL-rewriting software,²⁰ SPF, DKIM,²¹ and DMARC.²² Every state had at least one form of email protection in place.

Tabletop Exercises

Tabletop exercises (TTXs) are a best practice and increasingly popular method for training election officials and other VRDB users. TTXs place participants in scenarios that simulate some of the worst events that could occur during an election cycle. A cyberattack that cripples a VRDB, a misinformation campaign aimed at confusing voters, and a terrorist attack on a polling place are a few examples of scenarios that could be simulated during a TTX. States, the federal government, and other organizations have realized how powerful TTXs can be when training real-world preparedness. Just this year, several

---

¹⁹ Three states claimed to only teach some of their users about this threat. Only one state reported not teaching any users.
²⁰ URL-rewriting software rewrites any links found in an email. Then, when a user clicks a link, the user is redirected to an intermediary site that will restrict access to the destination site if that site is known to be malicious. Gil Friedrich. "Link Rewrites: The Good, The Bad, and The Over-Promised." Avanan. Accessed September 19, 2018. https://www.avanan.com/resources/link-rewrites.
²² DMARC is a newer form of email protection that ensures SPF and DKIM are working properly and protects against certain threats that take advantage of weaknesses in SPF and DKIM. See id.
prominent TTXs were held by DHS,\textsuperscript{23} the Belfer Center,\textsuperscript{24} and several states.\textsuperscript{25} Over half of surveyed states reported that they involve some or all of their VRDB users in tabletop exercises.

Who trains using tabletop exercises?

\begin{center}
\begin{tabular}{|c|c|c|}
\hline
 & All users & Some users & Not used \\
\hline
8 & 8 & 11 \\
\hline
\end{tabular}
\end{center}

As the nature of the cybersecurity landscape is constantly evolving, the frequency of cybersecurity training is becoming increasingly important. Almost every responding state reported engaging in cybersecurity training, and the survey found that twenty-one states conduct cybersecurity training at least once per year. Five other states reported that they also conduct cybersecurity training, but not as regularly.

Detection

No matter how many security measures are in place, no system is completely unhackable. Thus, in addition to preventative measures, it is important to be able to detect and respond to threats on an ongoing basis.

Monitoring

An important detection measure is monitoring attempts to login to the VRDB, either successful, unsuccessful, or both. Over two-thirds of responding states reported monitoring login attempts, fifteen of which reported monitoring both successful and unsuccessful login attempts.\textsuperscript{26}

\begin{center}
\textbf{Login Attempts Monitored}
\end{center}

\begin{center}
\begin{tabular}{|c|c|c|}
\hline
 & Successful and Failed Attempts & Only Failed Attempts & Login Attempts Not Monitored \\
\hline
15 & 5 & 6 \\
\hline
\end{tabular}
\end{center}

Another way malicious actors can threaten VRDBs is by attempting to inject database commands or other code in an effort to alter the database or to escape from the database

\begin{itemize}
\item \textsuperscript{24} "Officials from 38 States Learn to Fortify Elections Against Attacks." Belfer Center Newsletter. Belfer Center for Science and International Affairs, Harvard Kennedy School (Spring 2018).
\item \textsuperscript{26} Another six states reportedly did not monitor or audit any login attempts.
\end{itemize}
and obtain administrative access to the backend. In fact, that is exactly how Illinois’s VRDB was compromised in 2016. Twenty-seven states that do not monitor for unauthorized or abnormal database queries and/or improperly formatted inputs. Among states that do not monitor inputs, five have audited their input forms and API endpoints to ensure that only permitted inputs are accepted.

## Actions Taken to Protect Online Forms & API Endpoints

- Monitor for abnormal queries
- Monitor for abnormal queries & other signs of injection attack
- Audit to ensure only proper input allowed
- Don't know
- Other

Another common factor to monitor is change in traffic over time. It is important to know when VRDB traffic volume deviates from past trends so that states can investigate the source of the change. An increase in VRDB traffic could be innocuous, like when a voter registration drive registers a large number of people all at once. However, an increase in traffic could also be the result of intruders. Eighteen states report monitoring all VRDB traffic as compared to expected volume of traffic over time. One state reported monitoring high-profile records, such as celebrities’ records, which can provide an early warning sign of VRDB tampering.

## Automatic Alerts & Auditing

Threats to a VRDB can be detected using a system that constantly monitors the VRDB and sends an automatic alert in case of suspicious activity, or by audits conducted afterward. Eighteen of the states that responded indicated having a system in place that automatically alerts them of irregular VRDB activity. Albert sensors, managed and monitored by the Center for Internet Security's Security Operations CERT. Accessed September 19, 2018. [https://www.us-cert.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf](https://www.us-cert.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf).


28 In this context, an endpoint is simply the final destination of data, like voter data, that has been communicated from a database to a user. An API, or application programming interface, is software that allows data to pass between two disconnected systems, such as a state VRDB and a county’s election administration software. Thus, an API endpoint is where data enters or leaves the API.
Center (CIS SOC), are added to states’ networks and high-performance intrusion detection software to detect malicious activity and potential threats so that states can be notified. The majority of respondent states use Albert sensors, while four other states use comparable third-party solutions to monitor their VRDBs. Additionally, according to DHS Secretary Kirstjen Nielsen, by the 2018 midterm elections, “more than 90 percent of registered voters will live in an area where [Albert sensors] are deployed on their election infrastructure.”

In addition to employing automatic threat detection, all but one of the responding states said they conduct audits to better understand the traffic to their VRDB. Of those states, eighteen conduct audits at least every three months, and thirteen conduct audits as regularly as every thirty days.

VRDB Traffic Audit Frequency

![VRDB Traffic Audit Frequency](chart.png)

**VRDB Monitoring Solutions**

<table>
<thead>
<tr>
<th>Solution</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albert Sensors</td>
<td>18</td>
</tr>
<tr>
<td>Third-party solution</td>
<td>4</td>
</tr>
<tr>
<td>In Development</td>
<td>1</td>
</tr>
<tr>
<td>None/Don’t Know</td>
<td>4</td>
</tr>
</tbody>
</table>

---

30 "Albert." Center for Internet Security. Accessed September 19, 2018. [https://www.cisecurity.org/services/albert/](https://www.cisecurity.org/services/albert/). CIS SOC manually reviews anomalies for every 24 hours of monitoring. So, while not a real-time threat detection tool, Albert sensors still provide threat detection that is automatic from the state’s point of view.

**State Highlights: Illinois**

In 2016, while several states were targeted, Illinois was the only state that experienced an actual breach. The attackers injected SQL database queries into a vulnerable form on a public website, allowing them to gain access to voter records. Due to the methodical way the VRDB was infiltrated, the state didn’t detect the breach for three weeks, when the intruders accessed many more records than they had previously, resulting in a performance drop in the system. Later, it was revealed that tens of thousands of Illinois voters’ records were viewed by the intruders during this incident. Fortunately, Illinois, as well as many other states, has worked tirelessly to improve their VRDB security since then.

Overall, Illinois is now one of the states with the best security practices. The state said they audit their systems at least once a month, which includes an analysis of VRDB traffic. They also back up their VRDB daily, and test those backups at least once a week. Illinois monitors failed login attempts—a common way intruders try to gain access to vulnerable systems. Additionally, the state has secured their VRDB input forms and API endpoints by auditing its systems to ensure those forms and endpoints only accept certain inputs.

Illinois has also deployed a variety of other security services and technologies. CIS’s Albert sensors provide regular monitoring of Illinois’s VRDB traffic. The state also uses DDoS mitigation tools to prevent attacks aimed at overwhelming their VRDB. As can be seen just from the results of this brief survey, Illinois has taken a number of steps to better secure their VRDB and harden it to future attacks.

**Mitigation**

If all else fails and an attack successfully alters or impedes a VRDB, then there must be a plan to both restore the system and, in the meantime, ensure elections continue to be administered properly. Backups are an easy way to restore a system after it has been compromised. However, despite the effectiveness of backups, contingency plans still play a big role in security planning.

Creating regular VRDB backups is perhaps the best insurance against permanent loss of voter data. Every respondent state indicated they regularly back up their VRDB. The vast majority of states reported that they perform backups every day. Additionally, over 90% of those states regularly test their backups to ensure they work, with many testing as frequently as every week.
Another way states can be prepared in case of their VRDBs are compromised—particularly on Election Day—is through the use of pollbook backups and provisional ballots. Mitigation techniques vary based on the types of pollbooks each state uses. Of the twenty-five states that responded, twenty use pollbooks that are never connected to their VRDB during polling hours. Five states reported using pollbooks that are either “sometimes” or “continuously” connected to their VRDB during polling hours. However, just two of those states use only pollbooks that are continuously connected. Additionally, all states with electronic pollbooks supported at the state level either require or advise local election officials to keep paper pollbooks as backups and/or have (or be able to produce) enough provisional ballots for all registered voters who may vote at a given location.

32 Under the Help America Vote Act, individuals must be allowed to cast provisional ballots if they declare they are registered and eligible to vote in the jurisdiction despite not being on the voter list or being deemed otherwise ineligible. 52 U.S.C. § 21082(a).

33 This includes paper pollbooks.

34 Of those five states, two used pollbooks that were “sometimes” connected and three used pollbooks that were “continuously” connected.

Conclusion

In 2016, several states’ VRDBs were scanned and one state’s VRDB was successfully infiltrated. The states are working harder now than ever before to make sure their election infrastructure is secure against the threat of foreign interference. Based on the survey responses, it’s clear that much progress has been made in securing VRDBs, though there’s still significant room for improvement. States are engaged in a number of positive security practices, like regular auditing systems and creating (and testing) VRDB backups. However, the states could improve in areas like password security and use of multi-factor authentication. Ultimately, the states are showing that they are serious about cybersecurity and will do everything in their power to fight back against interference in our democracy.