Voter Registration Database Security

August 2020

A report from

The Center for Election Innovation & Research

Who we are

The Center for Election Innovation & Research (CEIR) is a nonpartisan non-profit with a proven track record of working with election officials from around the country and from both sides of the aisle. We seek to build voter trust and confidence, increase voter participation, and improve the efficiency of election administration.

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

During the last presidential election year, foreign adversaries waged disinformation campaigns and, in a small number of cases, infiltrated voter registration databases (VRDBs). Now, there are a growing number of reports raising the specter of another presidential election that will be conducted under the shadow of extensive foreign interference campaigns. In 2016, the Russian government was the predominant adversary seeking to interfere with U.S. elections. This year, China and Iran have joined Russia as potential threats to the integrity of our nation's elections. We can—and should—expect attacks on election infrastructure and other attempts to undermine voter confidence. Fortunately, election officials have continued to work tirelessly over the last few years, meaning this year's election will be the most secure election in recent history.

The Center for Election Innovation & Research (CEIR) conducts a biannual survey to assess the state of voter registration database security (VRDB) in the U.S. The survey looks at three major areas of VRDB security: prevention, detection, and mitigation. The responses to the inaugural survey in 2018 showed that, in the wake of heightened awareness and concern over foreign interference in elections, the states were taking VRDB security seriously. However, there was still room for improvement, particularly with regard to VRDB user access requirements and efforts to prevent phishing.

CEIR confirms that the states continue to improve their practices, with several states making great strides in the last two years. Compared to 2018, almost twice as many states now require multi-factor authentication and passwords that are at least eight characters long. Nearly all states are monitoring all VRDB log in attempts, and while the states were already regularly backing up their VRDBs in 2018, this year's survey shows that most states are backing up their VRDBs on a daily basis. Additionally, VRDB users are receiving the training they need; nearly every state trains users on how to identify cyberthreats, and every state uses tabletop exercises to learn how to respond to real-world scenarios.

However, there is still room for improvement. Six states indicated they still do not use multi-factor authentication to restrict access to their VRDBs. Several states also need to improve their monitoring and auditing practices. For instance, there are still a small minority of states that do not monitor or audit their VRDB data input forms to protect against malicious input. Ultimately, however, the states are making significant strides toward improving their VRDB security, a trend we expect to see continue in 2022.

Introduction

The threat of foreign interference in U.S. elections is real. In 2016, the Russian government interfered with election infrastructure. Experts agree that the likely goal of this interference was not to change actual votes, but to undermine Americans' confidence in their own democratic institutions and election processes.[1] To accomplish this goal, foreign adversaries mounted widespread disinformation campaigns and in a small number of cases successfully infiltrated voter registration databases (VRDB).[2] The possibility of VRDB tampering still exists in 2020, and efforts by foreign governments to interfere in U.S. elections are ongoing. A key goal of these attacks is to diminish voter confidence in our democratic system of elections.[3]

If an attack on a voter database were successful, provisional ballots and other backups could mitigate much of the risk to vote casting and counting. However, the damage could still be significant. The alarm and confusion caused could lead to long lines, additional stress on poll workers, and frustration for voters. Such complications would likely further erode Americans' declining faith in our elections. Ensuring the integrity of each state's VRDB is key to rebuilding voter trust and confidence.

While some sources provide best practices for VRDB protection, the Center for Election Innovation & Research (CEIR) conducts a biannual survey to assess the state of VRDB security in the U.S.[4] This year's survey consisted of 22 questions addressing three major areas of cybersecurity: prevention, detection, and mitigation.[5] The survey was sent to the chief election officials in all 50 states and the District of Columbia. Of those, 30 states

---

1 Office of the Director of National Intelligence. Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution. Washington, DC: National Intelligence Council, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

2 *Ibid*; U.S. Congress. Senate. Select Committee on Intelligence. Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations. 115th Cong., 2d sess., May 8, 2018. S. Rep. https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

3 Office of the Director of National Intelligence. Statement by NCSC Director William Evanina: 100 Days Until Election 2020. Washington, DC, July 24, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020.

4 See for example, Center for Internet Security. "A Handbook for Elections Infrastructure Security." Center for Internet Security. Accessed September 19, 2018. https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

5 Of the 22 questions, 21 were designed to track developments in the state of VRDB security by either copying or slightly adapting the language of the 2018 survey for clarity. The final question was left open-ended for respondents to volunteer observations concerning changes in their state's VRDB security measures. The responses accepted as part of our survey were more limited in 2020, omitting "I don't know" from the list of possible selections. The survey instrument can be found in Appendix A, located at the end of this report.

submitted responses.[6] Twenty states, or more than two-thirds of our respondents from 2020, also participated in 2018, allowing us to track the evolution of modern VRDB security protocols.

This report details the results of the 2020 VRDB security survey, comparing them with those from 2018. It also contextualizes the importance of key security measures to ensure the integrity of VRDBs. To preserve cybersecurity and prevent adversaries from using this information to refine their attacks on particular states, we do not identify the states that responded to the survey, and we only report on aggregated responses and trends.[7]

6 Regardless of its status as a state, commonwealth, or district, each survey respondent is anonymously referred to as a "state." Some states declined to answer questions due to security considerations. Those states' answers are included in the analysis of the questions to which they responded, sometimes impacting the denominators of our statistics. Two states declined to participate in the survey and are not included in this report.

7 CEIR received express written permission to include the few states that are named in this report.

VRDB Security in 2020

This report covers the current state of VRDB security with a special focus on tracking improvement since 2018. First, we examine how VRDBs are designed and maintained to prevent attacks by controlling access, promoting system integrity, and training users. Next, we address threat detection through real-time monitoring and audits. Finally, we consider state efforts to mitigate the impact of successful attacks on their VRDBs.

Prevention

The first step toward securing any electronic system is limiting vulnerabilities. Preventing unauthorized access to VRDBs and the sensitive information they contain requires controlling access, using secure tools and services, regularly auditing and maintaining systems, and training users to appreciate and avoid cyberthreats. In this way, prevention is two-fold, consisting of both digital and human elements.

Access

Effectively controlling access is an important preventative measure for securing the centralized statewide VRDBs used today.[8] Although not all VRDBs are designed the same way, each contains sensitive voter information. Users have various reasons for needing access to their state's VRDB, 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 a VRDB.[9]

Passwords

Using strong passwords has long been considered one of the most important ways to secure access to any electronic system, including VRDBs. Passwords may have various requirements regarding length, character variety, or how frequently they must be changed. In 2018, 13 of 25 responding states reported their user passwords were required to meet at least two conditions, such as using a minimum of 10 characters, including at least three different character types, not matching a common password such as "password" or "12345," or some other additional criteria. Our data from 2020 indicates that several states have instituted additional password requirements since 2018. Out of 28 respondent states, 20 require passwords that meet all of the following criteria: a minimum number of

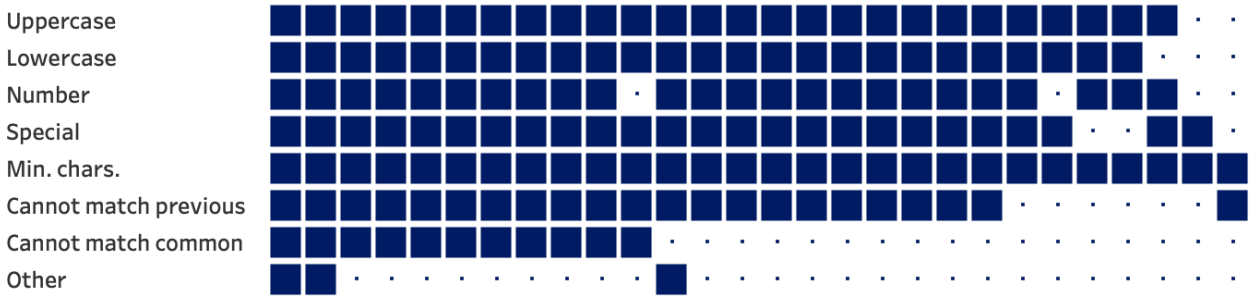
8 In this context, "access" is used broadly, referring to both the ability to retrieve and manipulate data.

9 This section mainly focuses on securing rather than limiting access. Our 2018 survey found that all responding states varied access privileges among different types of users, a best practice for VRDB security. See David Becker et al. "Voter Registration Database Security." Washington, DC: The Center for Election Innovation and Research, September 2018. https://electioninnovation.org/2018-vrdb-security/.

characters, at least one uppercase and one lowercase letter, at least one number and one special character, and a password that does not match one previously used. All but one state required a minimum number of characters, ranging from six to 16 characters with a median of eight.

However, the consensus about what constitutes a strong password has shifted in recent years. According to the National Institute of Standards and Technology's (NIST) guidelines, requiring complex passwords (with various character types) and forcing users to regularly change their passwords may no longer be a security best practice.[10] On the other hand, NIST's guidelines support requiring passwords to be at least eight characters long. In 2018, only 13 of the 25 responding states met this guideline. Since that time, out of the 27 states that reported their password length requirements in 2020, 25 now require the eight-character minimum. Of the 18 that responded both years, seven states have now changed their requirements to meet the eight-character recommendation.

Password Requirements, States that Responded in 2020



Note: Each column represents one state's responses, for a total of 28 responding states.

Multi-factor Authentication

Multi-factor authentication (MFA) goes hand-in-hand with password security and helps ensure only authorized users gain access to a system.[11] To verify a user's identity, MFA typically requires the use of a password and a secondary physical, digital, or biometric

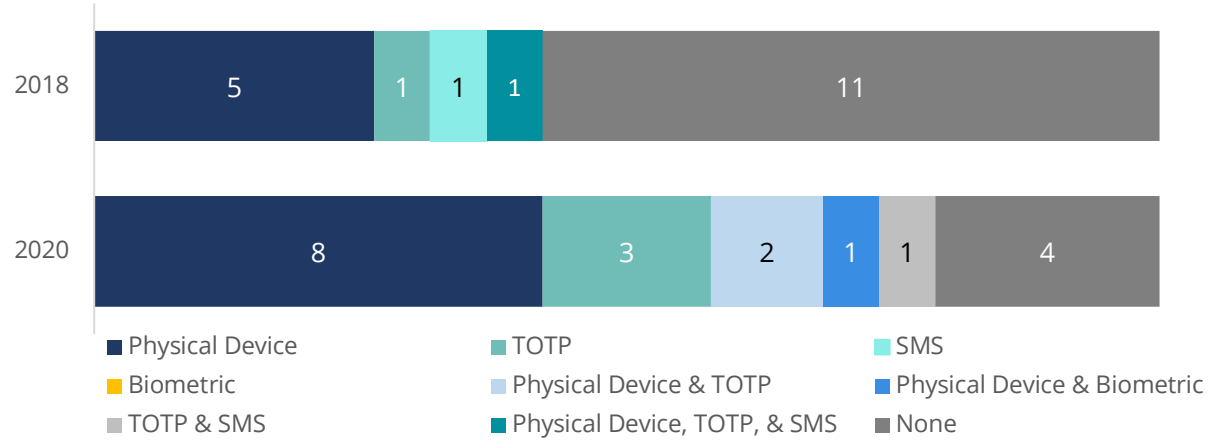
10 These requirements make passwords harder to remember, which frustrates users who then take insecure shortcuts (e.g., by writing passwords down or only making minor changes). Paul A. Grassi et al. "Digital Identity Guidelines: Authentication and Lifecycle Management." Special Publication 800-63B. Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce, June 2, 2017, updated March 2, 2020. https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

11 Jack Gillum and Jessica Huseman. "The Overlooked Weak Link in Election Security." ProPublica, September 14, 2018. https://www.propublica.org/article/the-overlooked-weak-link-in-election-security?token=k0PuAmvq_Xy63TS9ofcxNn6J431eO1RK.

authentication factor.[12] By requiring a second authentication step in addition to providing a traditional password, MFA can help combat phishing and other common threats that seek to obtain and exploit users' login credentials or other personal information to gain unauthorized access to a system.[13]

Among the 19 states that responded to questions about their MFA use in both 2018 and 2020, there has been demonstrable improvement. While in 2018 only eight of these states required MFA, by 2020 that number had nearly doubled to 15 states. Among the 29 states that responded this year, 23 reported they require MFA. Physical devices were the most popular secondary authentication factor among 2020 respondents (used in 15 states), followed by time-based one-time passwords, or TOTP (used in 10 states). Seven states reported using both of these.

Multi-factor Authentication, States that Responded in 2018 and 2020



System Integrity

Beyond securing access, states should have measures in place to maintain VRDB system integrity and prevent cyberattacks on an ongoing basis. To do that, VRDBs and connected systems must be designed to account for users' security shortcomings. While no one measure can ensure a system's integrity, the combination of various security measures, knowledgeable system administrators and IT staff, and regular system maintenance can help fortify VRDBs against the threat of outside attack.

---

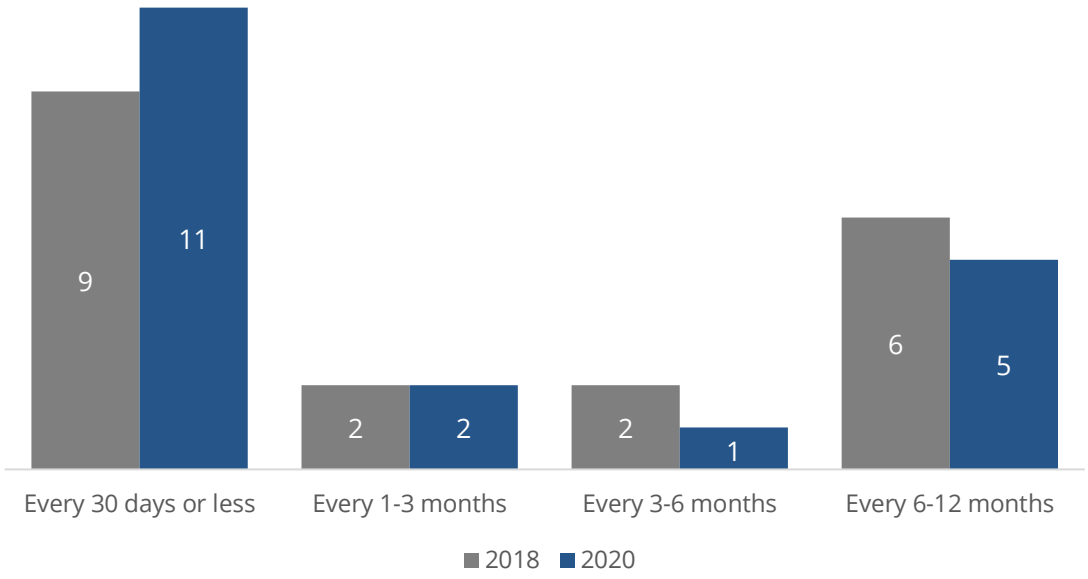
12 "Multi-Factor Authentication." Cybersecurity and Infrastructure Security Agency, March 25, 2019. https://www.cisa.gov/sites/default/files/publications/cisa-multi-factor-authentication.pdf.

13 Phishing and spear-phishing are common cyberthreats that target the human side of VRDB security by attempting to trick people into divulging personal information through the use of fraudulent emails or other communications. Cybersecurity and Infrastructure Security Agency. "Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks," March 11, 2020. https://us-cert.cisa.gov/ncas/tips/ST04-014.

System Audits

Like any system exposed to the internet, after a VRDB is created, it should be audited regularly to ensure that it is functioning fully and securely. This is another area of strength for the states. The 2020 survey found that 27 out of 29 respondent states currently conduct systems audits, though the frequency with which these audits are conducted can vary greatly: some states audited their systems at least monthly while others performed audits less than once per year. Among the 19 states that responded to this question in both 2018 and 2020, all 19 have continued to conduct systems audits. Additionally, among those same states, more states reported that they conduct these audits on at least a monthly basis compared to 2018.

Systems Audit Frequency, States that Responded in 2018 and 2020



IT Support

Experienced IT staff ordinarily handle the administration and maintenance of VRDBs and related systems. In 2020, every responding state reported having access to full-time IT support for their VRDB: eight reported they have a contract with outside IT professionals, and the remaining 21 reported they receive in-house support from at least one staff member. Among the 18 states that responded in both 2018 and 2020, each state had full-time support both years, although three states shifted from using in-house support in 2018 to outside professionals in 2020.

Threat Awareness & Targeted Attack Protection

Just as a system needs to be designed to prevent human error, users must also be trained to minimize vulnerabilities. Even the most secure system can be compromised if a

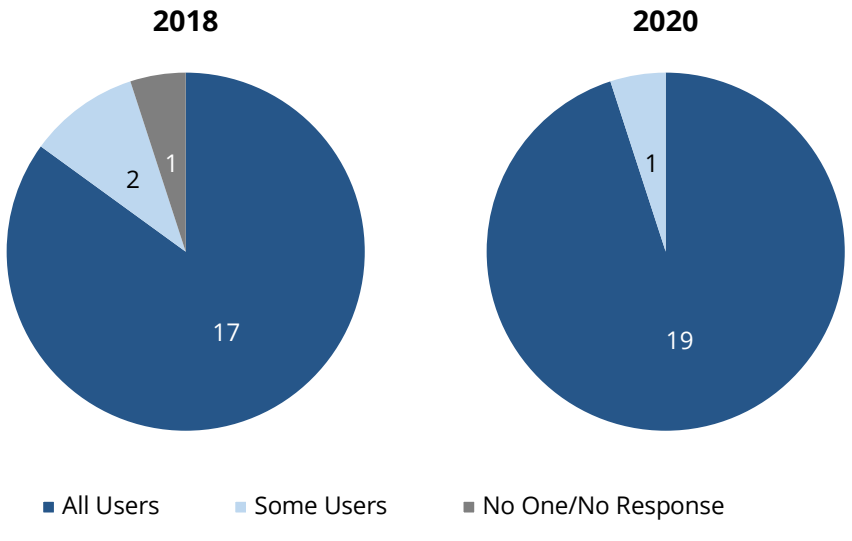
user shares their credentials or engages in other risky practices. VRDB users must be trained to watch for the cyberthreats they might encounter. States are managing many aspects of their VRDB users' training and communication effectively.

User Training

In 2020, 29 out of 30 states reported they train authorized VRDB users to identify cyber threats. The frequency of cybersecurity training is also becoming increasingly important to keep up with the constantly evolving field of cybersecurity. Of the 29 states that responded this year, 28 reported they conduct cybersecurity training at least annually. Of the 20 states that responded to both the 2018 and 2020 surveys, five states have increased the frequency of their training and the remaining 15 have maintained their frequency.

One of the most pressing problems in security today is the prevalence of phishing, a technique which can trick even the most careful users into handing over their login credentials. All 2020 respondent states reported training VRDB users specifically to recognize phishing and spear-phishing. In the vast majority of states, all users participate in this training, though in two states, only some users were trained on this threat. Nineteen of the 20 states that responded to both the 2018 and 2020 surveys reported all users were trained to recognize phishing and spear-phishing.[14] Despite all states training users on this threat, the survey showed that, since 2018, one state has reduced the number of users who receive this training, while three states have increased the number of users being trained.

Users Trained to Recognize Phishing, States that Responded in 2018 and 2020



14 One state reported only certain users receive this training.

State Highlights: Idaho

A recent study found that less than half of America's local election officials use even basic protections to ward off the threat of phishing.[i] With the now ever-present threat of election interference looming, it is imperative that election officials know how to confront common adversarial tactics, such as phishing and spearphishing. Fortunately, our survey showed that the states are ensuring users learn about phishing and know how to respond. A recent email exchange between CEIR and an election official in Idaho demonstrated that the state's training is working.

While preparing this report, CEIR followed up with several states to discuss their survey responses. Among those states was Idaho. To initiate our follow up, a CEIR staff member sent a cold email to an Idaho election official. Rather than immediately respond to what could be a phishing attempt, the official relied on the training that he and all other Idaho VRDB users receive on an annual basis. To make sure he was actually communicating with someone at CEIR—and not a bad actor—the Idaho official directly contacted CEIR's executive director, David Becker. After confirming the identity of the CEIR staff member who sent the email, the official was happy to connect CEIR with the resources we needed to complete our report.

i Area 1. Phishing Election Administrators. July 2020. https://cdn.area1security.com/reports/Area-1-Security-PhishingForElectionAdministrators.pdf

Tabletop Exercises

States also can train election administrators using tabletop exercises (TTXs), which place participants in scenarios that simulate some of the worst events that could occur during an election cycle.[15] Participants discuss the appropriate procedures to follow in a variety of circumstances and learn to act quickly in response to different crises. All 30 states that responded in 2020 reported using TTXs as part of their cybersecurity training.

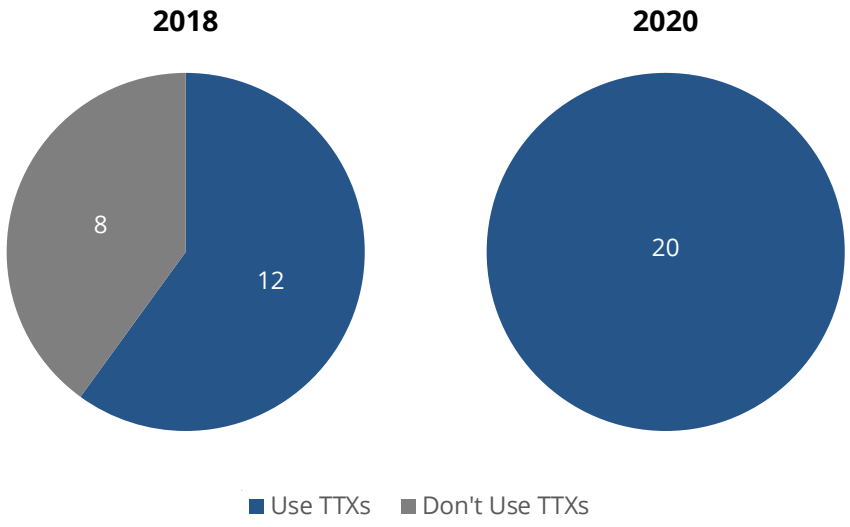
15 The Cybersecurity and Infrastructure Security Agency conducted its third annual Tabletop the Vote Exercise in July 2020, which included representatives from the federal government and 37 states. Cybersecurity and Infrastructure Security Agency. Federal, State, Local and Private Sector Partners Conduct Nationwide Exercise to Test Election Day Plans. Washington, DC, July 30, 2020. https://www.cisa.gov/news/2020/07/30/federal-state-local-and-private-sector-partners-conduct-nationwide-exercise-test.

CISA has created a situation manual for election officials to use that includes a variety of TTX scenarios, such as responding to a phishing campaign designed to gain access to a VRDB. Cybersecurity and Infrastructure Security Agency. Elections Cyber Tabletop Exercise Package: Situation Manual. Washington, DC: National Intelligence Council, January 2020. https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf.

Nineteen states reported hosting their own TTXs and 20 states said they participated in externally hosted exercises (ten states reported participating in both).

Of the states that responded in both 2018 and 2020, there was a significant increase in the use of these exercises. In 2018, 12 of 20 states said they used TTXs; in 2020, all 20 states used TTXs.[16]

Use of Tabletop Exercises (TTX), States that Responded in 2018 and 2020



Email Security

Email protections help prevent phishing attempts and block harmful email attachments that could lead to a VRDB being compromised. These protections usually verify an email's sender or check the contents of a message. In 2018 and 2020, all responding states had at least one form of email protection in place. In both years, almost every state reported using spam filters, many in combination with other email protections including URL-rewriting software, SPF, DKIM, and DMARC.[17,18] States also reported using a

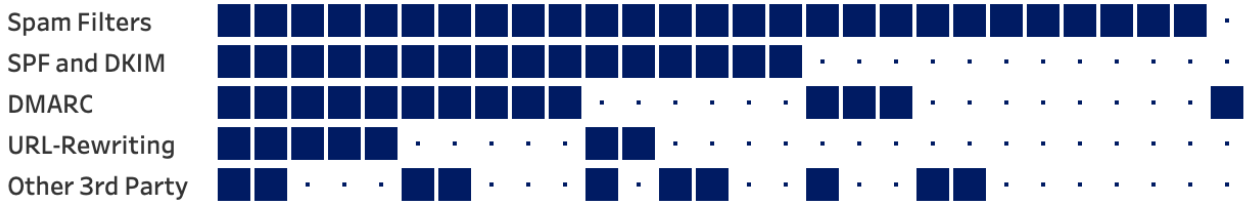
16 The 2018 survey did not ask states to distinguish between in-house and externally hosted TTXs.

17 URL-rewriting software rewrites links in emails to thwart phishing attempts. If a user opens a link that has been identified as malicious or is included on a list of blocked URLs, access is restricted. For more information concerning URL-rewriting software, see for example Microsoft's ATP Safe Links: Office 365. "Set up Office 365 ATP Safe Links Policies," June 8, 2020. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies.

18 SPF and DKIM are email authentication protocols that help prevent bad actors from impersonating a sender by establishing which IP addresses can send emails (SPF) and by creating a digital signature that mailbox providers can use to verify the sender's identity (DKIM). 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

variety of third-party services to provide firewalls and endpoint protections for their email systems.

Email Protections, States that Responded in 2020



Note: Each column represents one state's responses, for a total of 28 responding states.

Among states that responded in both 2018 and 2020, there has been clear improvement. Since 2018, one state started using spam filters. Nine states began using SPF and DKIM, however, one state stopped. Nine states started using DMARC, but one stopped. Four states implemented URL-rewriting. And five states started using other third-party email protections, but two states stopped using those protections.

Detection

No matter how many security measures are in place, no system is completely impervious to attack. In addition to preventative measures, it is important to be able to detect and respond to threats on an ongoing basis. On the whole, states report they are taking the right steps to monitor and audit their VRDBs effectively, though there continues to be room for improvement.

Examining VRDB Activity

Monitoring and auditing attempts to log in to a VRDB—whether successful or not—is an important measure to help detect malicious activity.[19] In 2018, 20 of 26 responding states reported monitoring login attempts. Fifteen of the states that responded in 2018 said they monitored both successful and unsuccessful attempts; though six states reportedly did not monitor or audit any. Among the 28 states that answered this year, all but two reported monitoring both successful and unsuccessful login attempts. Of the final two states, one monitored only failed attempts, while the other did not monitor either type

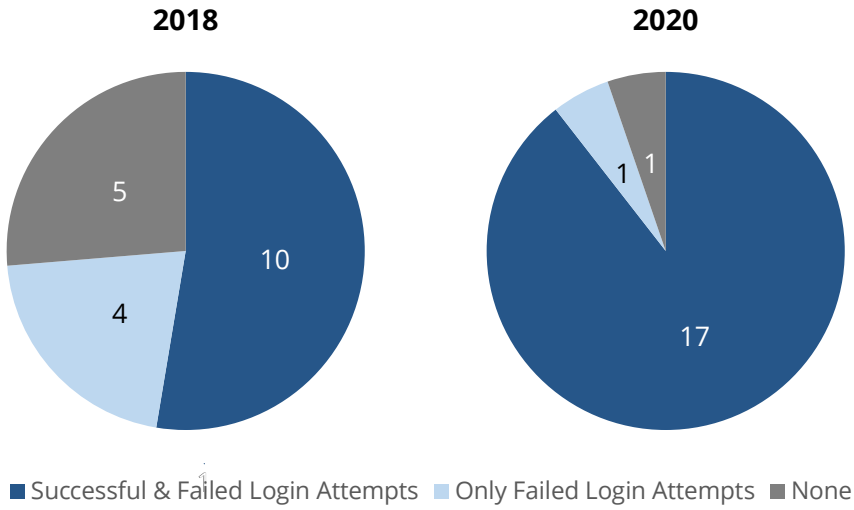
---

weaknesses in SPF and DKIM."DMARC Glossary." Glossary - DMARC Wiki. Accessed July 7, 2020. https://dmarc.org/wiki/Glossary; Indiana University. "About SPF, DKIM, and DMARC for Email Authentication." Knowledge Base, September 13, 2019. Accessed July 7, 2020. https://kb.iu.edu/d/azlu.

19 Monitoring and auditing are both ways of reviewing VRDB activity. The key difference between the two lies in the frequency of review. Monitoring is typically an ongoing process that often occurs in real time. Auditing occurs less frequently and usually involves a more in-depth, retroactive review.

of activity. Among the 19 states that responded in 2018 and 2020, four states moved from not monitoring either type of attempt to monitoring both successful and failed login attempts. Additionally, one state that did not previously conduct any monitoring began monitoring failed login attempts. Another three states switched from only monitoring failed attempts to monitoring and auditing all attempts.

Monitoring Login Attempts, States that Responded in 2018 and 2020



Malicious actors also threaten VRDBs by attempting to inject database commands or other code in an effort to alter the database or obtain administrative access to the backend. In 2018, 15 of the surveyed states said they monitor for unauthorized or abnormal database queries and/or improperly formatted inputs.[20] Among states that did not monitor inputs, five audited their input forms and API endpoints to ensure that only permitted inputs were accepted.[21]

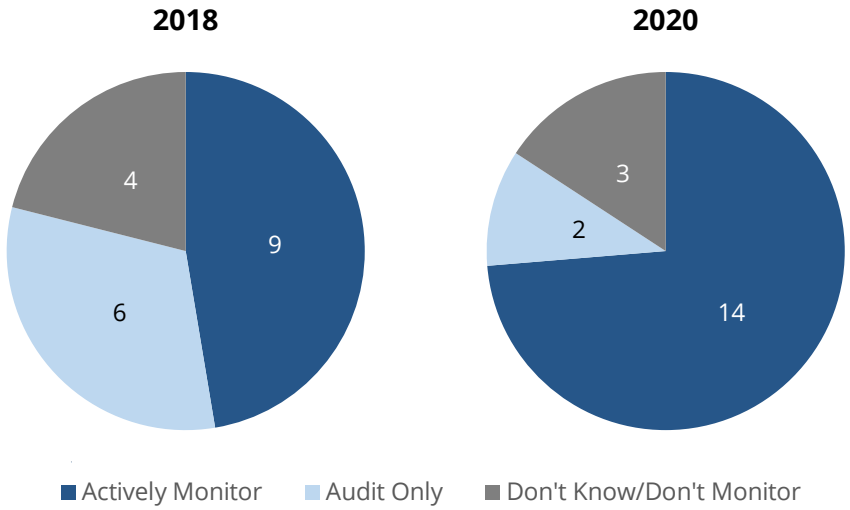
This year, 19 of the 24 states who responded to this question said they monitor for unauthorized or abnormal database queries and/or improperly formatted inputs. Three of the five remaining states have at least audited their input forms and API endpoints. Among the 19 states that responded in both 2018 and 2020, there was a slight overall

20 Improperly formatted inputs can be used to intentionally produce error messages, which can often provide attackers with important information about the system they are targeting. This is called an error-based SQL injection. Chad Dougherty. "Practical Identification of SQL Injection Vulnerabilities." Carnegie Mellon University, for United States Computer Emergency Readiness Team. Accessed July 7, 2020. https://us-cert.cisa.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf.

21 In this context, an "endpoint" is simply the final destination of data, like voter data, communicated from a database to a user. An API, or application programming interface, is a software intermediary that allows data to pass between two disconnected systems, such as a state VRDB and a county's election administration software. For this report, an "API endpoint" is the point where data enters or leaves an API.

improvement. Four states either started to monitor or expanded their monitoring of database queries and other inputs. However, one state indicated they no longer monitor this type of activity.

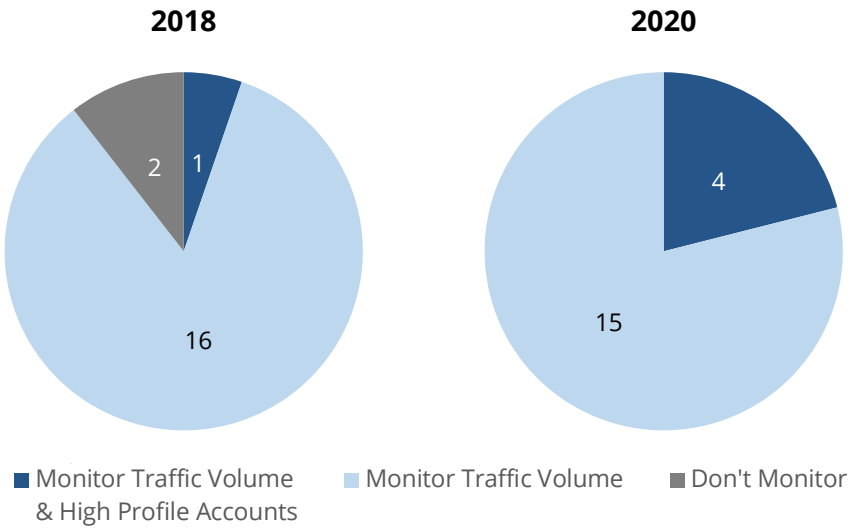
Monitoring Database Input Forms & API Endpoints, States that Responded in 2018 and 2020



Another common factor to monitor is change in traffic over time. It is important to know when VRDB activity 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 at once. However, an increase in traffic could also be the result of bad actors. In 2018, 18 of the 25 responding states reported monitoring all VRDB traffic to compare it with the expected volume of traffic. One state also reported monitoring high-profile records, such as celebrities' records, which can provide an early warning sign of VRDB tampering.

In 2020, 26 out of the 28 responding states reported monitoring their VRDB traffic volume. Four of those states said they also monitor high-profile records, such as celebrities' records, and one state reported monitoring user activity generally. Among the 19 states that responded in 2018 and 2020, six reported expanding their monitoring parameters and only one said they monitored fewer indicators in 2020 than they did in 2018.

Monitoring VRDB Traffic, States that Responded in 2018 and 2020



To effectively monitor change in VRDB traffic over time, states need to establish and regularly reassess their system performance baseline, considering metrics like traffic volume and how the system is used. To do this, states can perform an audit of their VRDB traffic. Among the 29 states that responded this year, the frequency of these audits varied considerably, ranging from at least once per month to less than annually. The most frequent response was "Every 30 days or less," but 13 states reported that they conduct less frequent traffic audits. Among the 19 states that responded both years, 16 either maintained or increased the frequency of their traffic audits. However, three states reported they moved to less frequent auditing.

Monitoring Systems

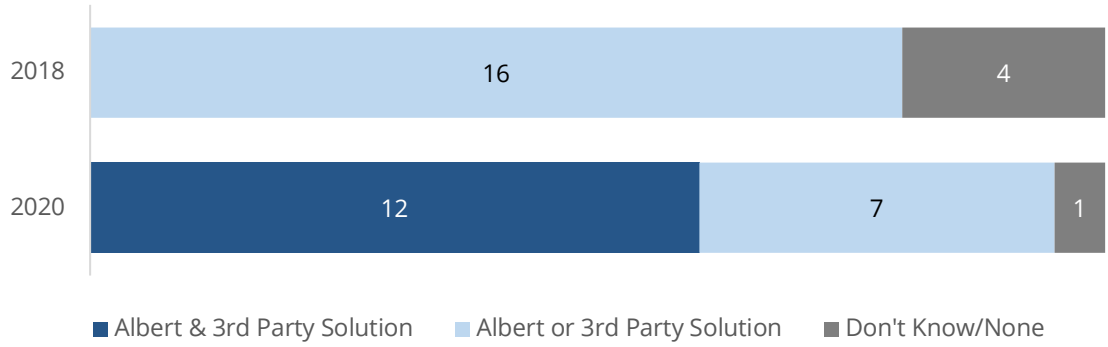
Active monitoring systems are a common tool used to detect threats to a VRDB. These systems constantly monitor external network traffic to either affirmatively prevent VRDB intrusions and/or alert IT staff about suspicious activity. This year, 26 out of 28 responding states indicated that they use a system that automatically alerts them to irregular VRDB activity. Eighteen of the 19 states that responded in both 2018 and 2020 reported using such a system. That was up from only 13 states in 2018.

Albert network monitoring is a monitoring solution offered exclusively to U.S. state, local, tribal, and territorial governments, and it works by pairing an intrusion detection system with real-time expert threat analysis.[22] Among the 20 states' progress we were able

22 Albert sensors are typically physical servers that are directly connected to government computer systems to monitor traffic. The Center for Internet Security manages the sensors and provides the monitoring services that detect potential threats to VRDBs and other systems. Center for Internet Security. "Albert Network Monitoring." Accessed July 7, 2020. https://www.cisecurity.org/services/albert-network-monitoring/.

to track, six have begun using one or more Albert sensors since 2018. This year alone, 27 out of 30 states reported using Albert sensors to monitor their VRDB.[23]

Monitoring Solutions, States that Responded in 2018 and 2020



Beyond Albert, states can also use a wide variety of third-party solutions to monitor their VRDBs.[24] States have substantially increased the use of these systems in the last two years. Out of the 19 states that answered both years, 16 originally stated they were either unsure or did not use third-party monitoring systems in 2018. Since then, nine of those states have begun using third-party monitoring solutions. From the full set of 2020 responses, 21 of the 29 respondent states reported using such monitoring systems.

Use of Third-Party Monitoring Solutions, States that Responded in 2018 and 2020

23 Of the three states that reported they do not use Albert sensors, one is currently working to set up Albert sensors while also using another third-party solution, one uses a third-party monitoring solution, and the last uses an Albert sensor for parts of their network beyond their VRDB.

24 Two commonly-used third-party monitoring solutions are Trustwave (https://www.trustwave.com/en-us/) and Microsoft Azure (https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/).

State Highlights: Virginia

From creating step-by-step security incident response plans to implementing automated security testing of software libraries, Virginia, like many states, has taken a comprehensive approach to confronting the challenge of securing its elections and election systems to promote integrity and voter confidence.

In 2019, Virginia enacted a new law aimed at increasing the security of its VRDB as well as other election systems.[i] That law, which went into effect on July 1, 2019, promotes the standardization of cybersecurity practices at the state and local levels, going so far as to permit the Department of Elections to restrict local access to Virginia's VRDB if a locality fails to meet minimum security requirements. To help local officials meet these new standards, the Department of Elections also increased the amount of training available for election officials, with a special focus on important topics like creating strong passwords, using multi-factor authentication, and identifying cyber threats.[ii]

Among the many improvements the state reported since our 2018 survey, Virginia now mandates the use of multi-factor authentication (using temporary one-time passwords) and further limits access to its VRDB by using IP whitelisting and geo-blocking. The Commonwealth also secures access by preventing user passwords from containing personal information and enforcing a minimum length requirement that is greater than most other states reported. Additionally, Virginia now keeps a record of all sign in attempts (successful and failed), a significant improvement over 2018 when no sign in attempts were logged.

i H.B. 2178, Sess. of 2019, (Virginia 2019). https://lis.virginia.gov/cgi-bin/legp604.exe?191+sum+HB2178&191+sum+HB2178.

ii The Virginia Department of Elections. "News Release: The Virginia Department of Elections Highlights Security Initiatives to Ensure Election Integrity," February 27, 2020. https://www.elections.virginia.gov/new-releases/the-virginia-department-of-elections-highlights-security-initiatives-to-ensure-election-integrity.html.

Mitigation

When prevention efforts fail to block an attack, states must be ready to respond swiftly. Some resources, such as content distribution networks (CDNs) and distributed denial-of-service (DDoS) mitigation tools, can help ensure a VRDB remains available to authorized users even in the wake of an attack.[25] However, if all else fails and an attack

25 Most DDoS mitigation tools also play a role in preventing and detecting DDoS attacks while CDNs focus on mitigating rather than preventing or detecting attacks.

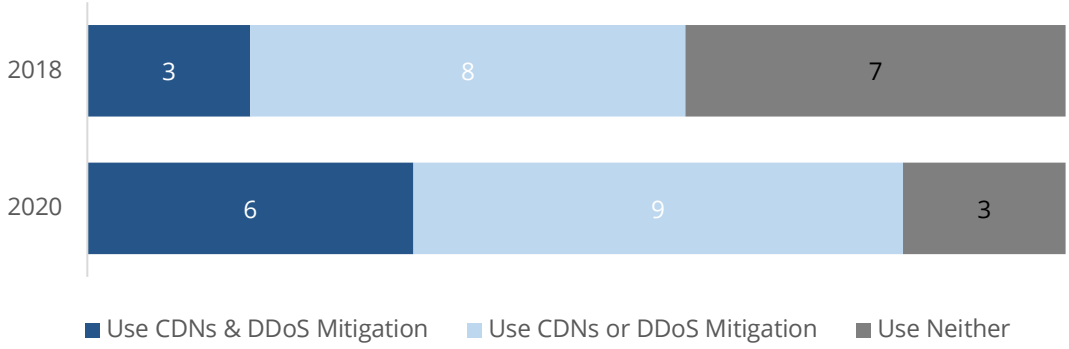
successfully alters or impedes a VRDB, there must be a plan to both restore the system and, in the meantime, ensure elections continue to be administered properly.

CDNs and DDoS Mitigation

DDoS attacks are a common way for malicious actors to disrupt legitimate users' access to a website or other networked computer system.[26] CDNs and DDoS mitigation tools can address these and other similar attacks. CDNs redundantly maintain content over several servers—useful in case a single server is overwhelmed or otherwise compromised.[27] Dedicated DDoS mitigation tools tend to be more focused in their approach. Typically, DDoS mitigation tools first analyze traffic patterns to establish an expected baseline, then redirect unusual traffic before it reaches its destination.[28] In practice, both CDNs and DDoS mitigation tools can be effective ways to ensure networked systems stay online and usable.

In 2018, 16 of the 25 responding states said they used either CDNs, DDoS mitigation tools, or both. In 2020, 21 of the 27 responding states reported using at least one of these systems. Nine of the 21 states use both. DDoS mitigation platforms remain the most popular, used by 19 of the states that responded. Among the 18 states that responded to this survey question in 2018 and 2020, six states that previously did not use either have since begun using at least one of these tools to help protect their VRDB.

Use of CDNs & DDoS Mitigation Tools, States that Responded in 2018 and 2020



26 DDoS attacks work by leveraging various sources of traffic to overwhelm the resources of a target. Cybersecurity and Infrastructure Security Agency. "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," November 20, 2019. Accessed July 7, 2020. https://us-cert.cisa.gov/ncas/tips/ST04-015.

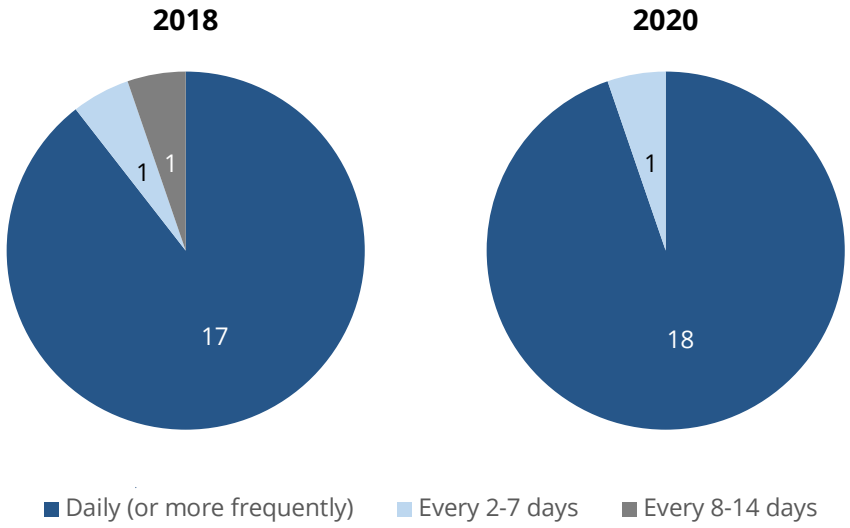
27 "What Is a CDN? How do CDNs Work?" Cloudflare. Accessed July 7, 2020. https://www.cloudflare.com/learning/cdn/what-is-a-cdn/.

28 "Security Tip (ST04-015): Understanding Denial-of-Service Attacks."

Backup and Contingency Plans

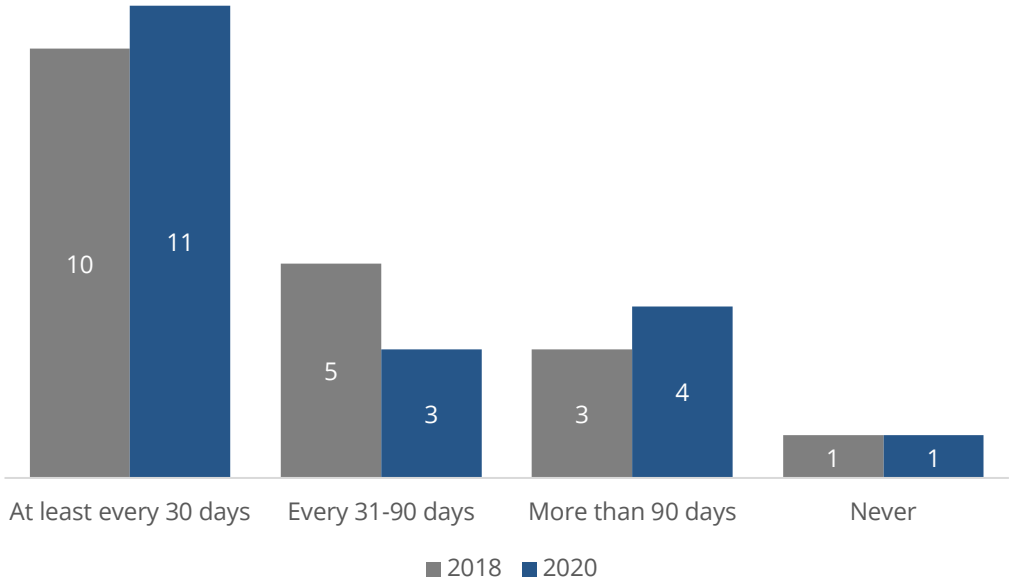
Creating regular VRDB backups is the best insurance against permanent loss of voter data. In 2018, every respondent state indicated they regularly backed up their VRDB. Twenty-three of 26 states reported they performed backups every day, and 24 states regularly tested their backups to ensure they worked. These rates held in 2020. All states that responded to the survey both years continue to back up their VRDBs. Two states that previously reported backing up their VRDBs less frequently have since moved to daily backups; however, one state reduced its backup frequency from daily to every two to seven days. Now, all but one out of 28 responding states back up their VRDB at least weekly, and 24 states do so every day.

VRDB Backup Frequency, States that Responded in 2018 and 2020



In 2018, 24 of 28 states regularly tested their backups to ensure they worked. This year, all but two responding states reported they test their backups, but the frequency of those tests varied significantly, ranging from at least once per week to less than once every 90 days. The 19 states that responded in 2018 and 2020 showed a slight decline in their testing frequency overall compared to 2018, but most states still tested at least once per month.

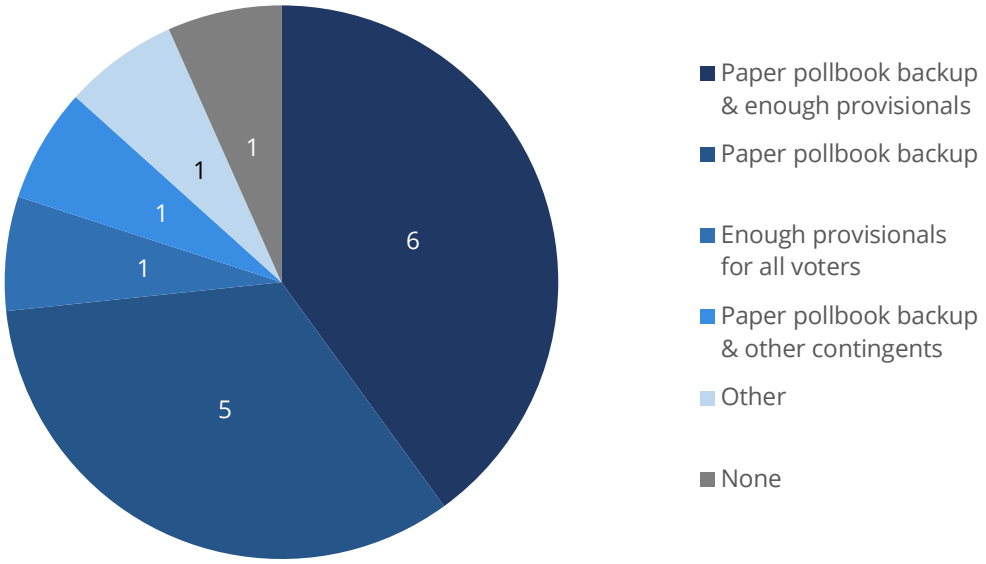
VRDB Backup Test Frequency, States that Responded in 2018 and 2020



States also can prepare for a possible Election Day VRDB attack by using pollbook backups and provisional ballots. Mitigation techniques vary based on the types of pollbooks each state uses, and states can use multiple types of pollbooks for a given election. Of the 25 states that responded in 2018, 20 used either paper pollbooks or electronic pollbooks that were never connected to their VRDB during polling hours. Two states reported using pollbooks that were sometimes connected, while three used pollbooks that were continuously connected. In 2020, 18 of 30 responding states reported using multiple types of pollbooks. Out of the full 30 states, 24 use paper pollbooks (five of those states only use paper pollbooks), and 21 use electronic pollbooks not connected to the VRDB during polling hours. Only six states use pollbooks that are sometimes or continually connected to the VRDB during polling hours.

All but one state that reported using electronic pollbooks in 2020 also reported they have a contingency plan in place should their electronic pollbooks fail. Contingency plans may include requiring polling places to have a paper copy of the pollbook, maintaining a sufficient number of provision ballots, or any number of other preventative measures. Among the 15 states that reported using electronic pollbooks in both 2018 and 2020, there was a slight increase in the use of paper pollbook backups and the requirement that polling places have a sufficient number of provisional ballots on hand. However, one state reported that they no longer require any contingencies to be in place for a possible electronic pollbook failure.

Electronic Pollbook Contingencies, States that Responded in 2020



Conclusion

Ensuring the security of voter registration databases is an ongoing battle, but the states have made substantial progress since 2016. In 2016, several states' VRDBs were scanned and at least one VRDB was successfully infiltrated. Our 2018 survey showed that states had already made significant improvements in the security of their election infrastructure. Since then, states have further secured their systems.

There has been clear progress across a number of measures in VRDB security since 2018. Password requirements are coming into line with industry best practices, and there has been a notable rise in the use of MFA. The human element of VRDB security is being emphasized, with states utilizing a number of training methods to teach their VRDB users about various cyber threats. States are also making a distinct effort to improve and maintain the integrity of their systems by conducting regular audits to ensure any holes in their security structure are proactively identified and closed.

Since 2018, there has also been improvement in the detection of cyber threats: eight states have expanded their monitoring of login attempts, and almost every state now audits traffic to their VRDB. However, the frequency of these audits varies dramatically, offering states an area in which they might improve their security practices in the future. Of those we could track from 2018 to 2020, six states say they now have begun using Albert sensors. In 2020, almost all states reported using Albert sensors and a majority said they are using similar third-party solutions, ensuring their VRDBs are monitored around the clock for indicators of malfeasance.

States also showed that they are taking the necessary steps to mitigate the impact of any successful attacks. Should anything happen to the VRDB or electronic pollbooks,

there must be a backup plan in place to minimize potential chaos. All states that responded to this year's survey said they regularly back up their VRDB. All but one state said they had a backup plan in case electronic pollbooks fail. While it is commendable that states have these backups in place, there is still room for further improvement. For instance, while all but two states reported they did in fact test their VRDB backups, the majority did so less than once per week. By backing up their VRDBs and testing backups frequently, states can ensure they are prepared for the worst-case scenario, year-round, but especially on Election Day.

Ultimately, the states' voter databases are as secure as they have ever been, and we expect to see further improvement in subsequent years. Election offices are serious about cybersecurity and are actively working to combat interference in our democracy. CEIR will continue to track the states progress with another round of surveys in 2022. In our future research, we aim to keep pace with emerging technologies and ever-evolving security best practices, so that we can compare states' security systems to the most up-to-date standards.

Appendix A

2020 VRDB Security Survey

Answer frequency is included in red next to each possible response.

A few notes about how to understand this data:

- Many questions permitted respondents to select all options that applied to them, so the sum of all answer frequencies will often exceed the total number of respondents
- Some respondents chose not to answer certain questions, so the sum of all answer frequencies for questions with mutually exclusive response options may be less than the total number of respondents
- Free response answers were omitted to avoid including information that may identify respondent states

1. Are users required to use multi-factor authentication when accessing systems?
    - Yes 23
    - No 5

   IF YES: What forms of authentication do users use in addition to a password? [select all that apply]

    - A physical device like a security token, grid card, or security key (yubikey or Feitian device) 16
    - Personal biometric data, like a fingerprint 1
    - SMS authentication 4
    - A secondary Time-based One-Time Password (TOTP) (often provided by mobile phone apps, e.g. Google Authenticator) 10

2. What requirements are in place for user passwords? [select all that apply]
    - Minimum number of characters required 28
    - Must use at least one uppercase letter 26
    - Must use at least one lowercase letter 25
    - Must use at least one number 24
    - Must use at least one special character 25
    - Cannot match a previously used password 22
    - Cannot match commonly used passwords (e.g., “password1234”) 11
    - Other: _____ 1
    - None of these 0

IF MINIMUM # OF CHARACTERS: What is the minimum number of characters required for user passwords? Range: 6-16

3. Are users required to change their password(s)?
    - Yes 26
    - No 3

IF YES: How frequently are users required to change their password(s)?

- Every 30 days or fewer 2
- Every 1-3 months 15
- Every 3-6 months 7
- Every 6-12 months 2
- Less frequently than once per year 0

4. What types of email protection do you have in place? [select all that apply]
    - Spam filters 27
    - URL-rewriting software (e.g., Proofpoint) 8
    - SPF and DKIM 16
    - DMARC 15
    - Other third party protections or services 8
    - None of these 0
    - Other 0

IF OTHER THIRD PARTY PROTECTIONS OR SERVICES: What third party protections or services do you use, and what protection do they provide?

IF OTHER: [please specify]

5. Do you have at least one designated IT staff member who is responsible for your VRDB?
    - Yes, we have a full-time IT staff member responsible for our VRDB 20
    - Yes, we have a part-time IT staff member responsible for our VRDB 0
    - No, but we contract with an outside party for full-time IT support for our VRDB 8
    - No, but we contract with an outside party for part-time IT support for our VRDB 0
    - No, we do not have skilled IT support for our VRDB 0

6. Do you conduct systems audits to identify possible security vulnerabilities?
    - Yes 27
    - No 2

IF YES: How frequently do you conduct systems audits?

- Every 30 days or less 12
- Every 1-3 months 5
- Every 3-6 months 2
- Every 6-12 months 7
- Less than once per year 0
- Sporadically but not on a regular schedule (e.g., after a cyber incident) 0
- Never 0

7. Are authorized users trained on how to identify cyber threats?
    - Yes 29
    - No 1

IF YES: How frequently does this training occur?

- At least annually 28
- Irregularly or occurs less than once per year 0

8. Do you engage in training specifically regarding phishing and spear-phishing?
    - Yes 30
    - No 0

IF YES: How frequently does this training occur?

- At least annually 30
- Irregularly or occurs less than once per year 0

IF YES: Who participates in this training?

- All users are taught about this threat 28
- Only certain users are taught about this threat 2

9. Do you conduct tabletop exercises for cybersecurity training?
    - Yes 30
    - No 0

IF YES: Who participates in these exercises?

- All users 11
- Only some users 19

IF YES: Are these exercises conducted in-house or hosted externally?

- Conducted in-house 11
- Hosted externally 12
- Other 0

IF OTHER: [please specify]

10. Do you monitor and audit login attempts to your VRDB?
    - Yes, both successful and failed login attempts are monitored and audited 26
    - Yes, but only failed login attempts are monitored and audited 1
    - No, login attempts are not monitored 1

11. How do you monitor the input forms and API endpoints that interact with your VRDB in order to protect against forms of malicious input (e.g., attempts to inject database commands or data, or attempts to escape out of the database and obtain administrative access to the backend)? [select all that apply]
    - We monitor unauthorized or anomalous data manipulation language (DML) statements and/or data definition language (DDL) statements 18
    - We monitor for the results of other successful input format injection attempts 13
    - We do not monitor input forms or API endpoints, but we have audited all our input forms and API endpoints to ensure that only permitted inputs are accepted 6
    - We do not monitor input forms or API endpoints that interact with our VRDB 8
    - Other 5

    IF OTHER: [please specify]

12. Do you monitor any other indicators of attempted malfeasance, such as the volume of traffic to your VRDB over time and compare that volume to expected traffic? [select all that apply]
    - Yes, we monitor the volume of VRDB traffic over time compared to expected traffic 24
    - Yes, we monitor high profile records (such as celebrities' or other public figures' voter registration records) for unexpected changes 4
    - Yes, we monitor some other indicator of attempted malfeasance (please specify): _____ 10
    - No, we do not monitor any other indicators of attempted malfeasance 0

13. Do you use content distribution networks (CDNs) or DDoS-mitigation platforms (e.g., Cloudflare's Athenian Project or Google's Project Shield) for your Voter Registration Database? [select all that apply]
    - Yes, we use CDNs 11
    - Yes, we use a DDoS-mitigation platform 19
    - No, we do not use either of these 6

14. How often do you conduct an audit to better understand the traffic to your VRDB? This includes analyzing data such as traffic volume, origin, type of activity, etc.
    - Every 30 days or less 14
    - Every 1-3 months 3
    - Every 3-6 months 3
    - Every 6-12 months 4
    - Less than once per year 0
    - Sporadically/not on a regular schedule (e.g., only after a cyber security incident) 3
    - Never 0

15. Do you have a system that automatically alerts you if irregular VRDB activity (e.g., database injection attempts, unusual VRDB traffic, high number of failed login attempts, etc.) is detected?
    - Yes, we are automatically alerted about irregular activity 26
    - No, we are not automatically alerted about irregular activity 2

16. Do you use one or more Albert sensors to monitor your VRDB?
    - Yes 27
    - No 3

17. Do you use another third-party network monitoring solution (e.g. Trustwave, Cisco Gateway) to monitor your VRDB?
    - Yes 21
    - No 8

IF YES: What third-party network monitoring solution do you use? [free response]

18. Do you backup your VRDB and related systems?
    - Yes 29
    - No 0

IF YES: How frequently?

- Daily (or more frequently) 24
- Every 2-7 days 3
- Every 8-14 days 0
- Every 15-30 days 0
- Every 31-60 days 1
- Every 61-90 days 0
- More than every 90 days 0

IF YES: How long are backups preserved before being deleted or overwritten?

- Daily (or more frequently) 1
- Weekly 6
- Monthly 4
- Every 6 Months 7
- Every Year 1
- Every 2 Years or more 3
- Backups are never deleted or overwritten 3

19. Do you test your VRDB backups to ensure they work?
    - Yes 27
    - No 2

IF YES: How frequently?

- Every 7 days (or more frequently) 9
- Every 8-14 days 0
- Every 15-30 days 3
- Every 31-60 days 4
- Every 61-90 days 3
- More than 90 days 7

20. What system or technology is used to check in voters? (select all that apply)
    - Paper pollbooks 24
    - Electronic pollbooks that are not connected to the VRDB during polling hours 23
    - Electronic pollbooks that are sometimes connected to the VRDB during polling hours 4
    - Electronic pollbooks that are continually connected to the VRDB during polling hours 5

21. If your electronic pollbooks fail on Election Day (due to compromise, hardware failure, etc.), do you have contingencies in place? (select all that apply)
    - Yes, we require or advise local election officials to keep a paper pollbook as backup 22
    - Yes, we require or advise local election officials to have on hand, or be able to produce, enough provisional ballots for all registered voters who may cast a ballot at a given location 12
    - Yes, we have some other contingency in place. Please describe the contingency briefly: _____ 5
    - No, we do not have any contingencies in place to address electronic pollbook failure 1
    - Not applicable, we use paper pollbooks 6

22. Has your state made any other changes or implemented new solutions in cybersecurity since 2016 that were not mentioned above? Please feel free to highlight these changes here: [Free Response]