Voter Registration Database Security in 2022

January 2023

A report from
The Center for Election Innovation & Research

Who We Are

The Center for Election Innovation & Research (CEIR) is a nonpartisan nonprofit that conducts elections research and works with election officials from around the country and both sides of the aisle to support elections that voters should—and do—trust. We seek to restore trust in the American election system and promote election procedures that encourage participation while ensuring election integrity and security.

Authors

Kristin Sullivan
Research Director

Kyle Yoder
Sr. Research Associate, Policy

Stefan Martinez-Ruiz
Sr. Research Associate, Data Analysis

Kyle Upchurch
Project Manager, Research

April Tan
Sr. Research Associate, Policy

Kira Flemke
Research Associate, Data Analysis

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.

Acknowledgments

We would like to thank Matt Masterson, Matt Bernhard, and Jenny Lovell for their contributions to the survey. We would also like to thank all the election officials who responded to our survey and engaged in additional conversations.

Table of Contents

Executive Summary

Under substantial scrutiny and amid a national environment of misinformation and distrust, election officials across the country successfully administered highly secure and accessible elections in 2020 and 2022. In order to secure election infrastructure against both foreign and domestic threats, many of these officials worked hard to improve cybersecurity practices in their state. One critical component of this effort was ensuring the security of state voter registration databases (VRDBs). Any disruption to a state VRDB could have serious consequences for the smooth operation of elections and thus, erode voter trust and confidence.

The Center for Election Innovation & Research (CEIR) conducts a biennial survey to assess the state of VRDB security in the U.S. The survey looks at three major areas of VRDB security: prevention, detection, and mitigation. Responses to the 2018 and 2020 surveys demonstrated the seriousness with which states take cybersecurity. They also demonstrated substantial progress in security practices from 2018 to 2020. In both years, CEIR identified several areas of strength alongside opportunities for growth. Most recently, in 2020, we cited the states' strength in implementing best practices around establishing password requirements, monitoring login attempts, backing up VRDBs, training users, and requiring tabletop exercises. While we noted growth in the use of multi-factor authentication (MFA) between 2018 and 2020, we saw room for improvement. Finally, we called for progress in monitoring and auditing VRDB activity.

In this report, we demonstrate that respondent states have largely maintained the best practices they adopted in previous years. In terms of prevention, detection, and mitigation, states reported similarly encouraging practices in 2022 and demonstrated growth in key areas when compared to 2020. In the 2020 report, we called for further adoption of MFA; that progress was evident in 2022. We also saw states adapt to changes in best practices for password requirements, bring more IT support in-house, and adopt additional email security.

Still, opportunities for growth remain. The 2020 report noted room for improvement in the frequency with which states monitor and audit VRDB traffic and login attempts, and that need for improvement remains. Elsewhere, it appears there may have been slight regression in terms of minimum character requirements for user passwords. This remains a best practice and we would expect to see growth in this area in the future.

The 2022 survey asked about two new topics: security procedures for remote third-party access and adherence to the 3-2-1 rule in backing up VRDB systems. Both areas show encouraging initial results, even though there is room for growth. Overall, despite a few areas in which states could improve their practices, after three surveys, CEIR remains encouraged by the state of VRDB security across the country.

Introduction

Amid intense pressure, election officials in states across the country helped administer a secure and successful election in 2022. Indeed, in a statement after the election, Jen Easterly, Director of the Cybersecurity & Infrastructure Security Agency, thanked election officials for their hard work securing the election, announcing that the federal agency saw "no evidence that any voting system deleted or lost votes, changed votes, or was any way compromised in any race in the country."[1] These efforts built upon the security successes of the 2020 election, which the Election Infrastructure Government Coordinating Council Executive Committee named the most secure in U.S. history.[2] Countless officials across the country have worked to ensure election security, and a critical component of that security is the prevention, detection, and mitigation of issues affecting state voter registration databases (VRDBs).[3]

The threat of bad actors gaining access to and disrupting VRDB operations should be taken seriously. While the potential for direct manipulation of voter records is troubling, even less acute damage to VRDB systems could interrupt normal election operations and lead to poor voter experiences, including long lines and inaccurate voter lists. These issues could further erode trust in election integrity. For that reason, government agencies like CISA and organizations like the Center for Internet Security provide resources and toolkits to help states improve their security posture.[4]

Since 2018, the Center for Election Innovation & Research (CEIR) has contributed to the security environment by surveying state officials to gain insight into VRDB security, demonstrate best practices, and highlight areas for improvement. In 2020, we published

[1] "Statement from CISA Director Easterly on the Security of the 2022 Elections," Cybersecurity and Infrastructure Security Agency, November 9, 2022. https://www.cisa.gov/news/2022/11/09/statement-cisa-director-easterly-security-2022-elections.

[2] "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," Cybersecurity and Infrastructure Security Agency, November 12, 2020. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

[3] The Help America Vote Act (HAVA) of 2002 requires that all states with voter registration implement "a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level…" (52 U.S.C. § 21083(a)). Today, every state that requires voter registration, plus the District of Columbia, has its own statewide VRDB. "Voter Registration Database Security," The Center for Election Innovation and Research, September 2018. https://electioninnovation.org/wp-content/uploads/2018/09/2018-VRDB-Security-Report.pdf.

[4] See: "Cybersecurity Toolkit to Protect Elections," Cybersecurity and Infrastructure Security Agency, accessed January 20, 2023. https://www.cisa.gov/cybersecurity-toolkit-protect-elections; "The EI-ISAC's Essential Guide to Election Security," Center for Internet Security, updated January 12, 2023. https://docs.cisecurity.org/en/latest/.

our second biennial report on VRDB security. That report concluded that, while there was still room to grow, states had made substantial progress since 2018.[5]

This report demonstrates that respondent states have largely maintained the best practices they adopted in previous years and VRDB security remains an area of strength in our elections. The report also highlights some areas for improvement and introduces insights into new topics not covered in the previous reports.

Methodology

CEIR sent the 2022 VRDB security survey, which contained 49 questions, to chief election officials in every state and the District of Columbia; nearly half (23) responded.[6] The analysis that follows examines the 2022 survey responses and compares them primarily with responses to the 2020 VRDB security survey. Of the states that responded in 2022, 19 also responded in 2020, allowing for longitudinal comparison within this subgroup. In order to identify longer-term trends, the analysis also occasionally examines results from the 2018 VRDB security survey. To preserve cybersecurity and prevent adversaries from using this information to refine their attacks, we do not identify the states that responded to the survey and report only on aggregated responses and trends.

We acknowledge that, without responses from all 50 states, there are limitations to what this survey can say about VRDB security across the country. States that responded to our surveys may be subject to self-selection bias, and responses from any single subset of states do not necessarily generalize to trends across all states. However, with nearly half of states responding, including a sizeable subset that responded to past surveys, this report can point to important strengths and weaknesses among responding states and identify trends over time that may speak to developments in the field. CEIR is confident that this report constitutes a robust assessment of state practices that can contribute to the understanding of VRDB security across the U.S.

[5] "Voter Registration Database Security," The Center for Election Innovation and Research, August 2020. https://electioninnovation.org/2020-vrdb-security-report/.

[6] This is slightly fewer than the 30 states that responded in 2020.

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 user access to the VRDB; ensuring system integrity through secure monitoring, audits, and system maintenance; training users to identify and respond to cyber threats; and implementing email security protocols. In this way, prevention is two-fold, consisting of both digital and human elements.

Controlling User Access

Controlling access is an important preventative measure for securing the centralized statewide VRDBs states use today.[7] Although not all VRDBs are designed the same way, each contains sensitive voter information. Users have various reasons for needing access to their state 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. Thus, it is imperative to properly manage user permissions and secure each instance in which a user gains VRDB access.

Passwords

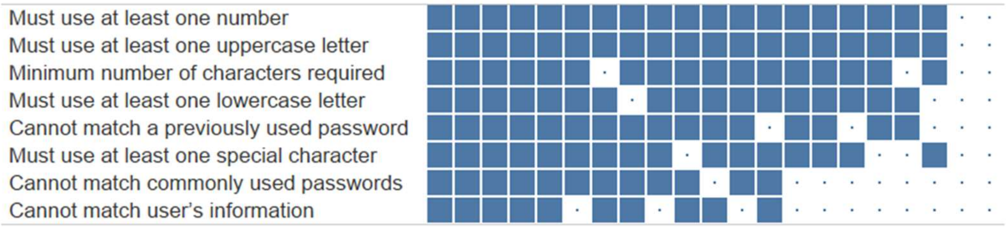
Using strong passwords has long been considered one of the most important ways to secure access to computer systems, including VRDBs. States may have various password requirements regarding length, character variety, or how frequently they must be changed. However, the consensus among cybersecurity experts about what constitutes a strong password has shifted in recent years. The National Institute of Standards and Technology's (NIST) guidelines advise against requiring either complex passwords (with various character types) or regular changes to user passwords.[8] These requirements make passwords harder to remember, which frustrates users who then take insecure shortcuts (e.g., by writing passwords down or making only minor changes).[9] States have nimbly adapted to meet the changing consensus around complex passwords. Of the 19 states that responded in both 2020 and 2022, 14 require passwords to contain a special character (e.g., '!' or '#') in 2022, down from 16 in 2020.

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

[8] 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, Sec. 5. https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

[9] Grassi, "Digital Identity Guidelines," Sec. 5.

Figure 1: Password Requirements: States that Responded in 2022



NIST guidelines do, however, support requiring passwords to be at least eight characters long.[10] In 2022, 17 of the 21 states indicated that they require user passwords to contain some minimum number of characters.[11] Of these states, 15 require passwords to be at least eight characters. Among the 17 states that responded to this question in both 2020 and 2022, the number of states that require some minimum number of characters for VRDB passwords decreased. In 2020, all 17 of those states required some minimum number of characters, but only 14 indicated the same in 2022. This decrease appears to reverse a trend that emerged between 2018 and 2020. In 2018, only 13 of the 25 responding states met the recommended guideline of an eight-character minimum, but in 2020, 23 out of the 25 responding states did so.

It is difficult to say if the moderate decrease in respondent states requiring a minimum password length is reflective of a broader trend. That said, given the NIST guidelines, we would expect to see more states adopt minimum length requirements in the future.

Multi-Factor Authentication

Multi-factor authentication (MFA) adds a layer on top of password security to help secure VRDB access.[12] To verify user identity, MFA typically requires the use of a password and a secondary physical, digital, or biometric authentication factor when accessing the VRDB.[13] 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 gain unauthorized

[10] Grassi, "Digital Identity Guidelines," Sec. 5.

[11] Two states chose not to respond to several questions. Thus, on occasion, we will report findings from fewer than 23 states. The total number of states we report can also change when comparing across years, for the same reason.

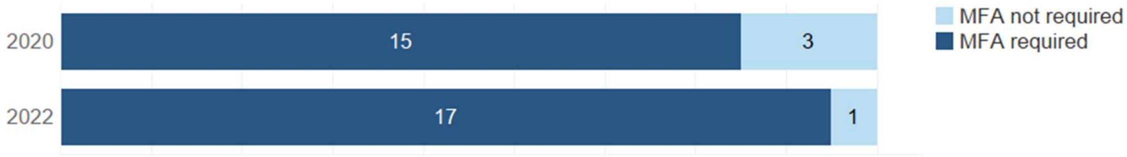
[12] "Multi-Factor Authentication," Cybersecurity and Infrastructure Security Agency, January 2022. https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf.

[13] CISA, "Multi-Factor Authentication."

system access by obtaining and exploiting user login credentials or other personal information.[14]

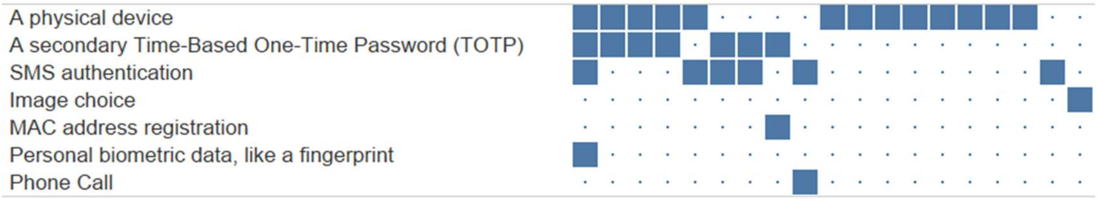
CEIR's 2020 VRDB security report called for further adoption of MFA among the states, and that progress is apparent this year. Among the 19 states that responded to this question in both 2018 and 2020, only eight required the use of MFA in 2018, while 15 did so in 2020. Among the 18 states that responded to this question in both 2020 and 2022, 17 reported requiring MFA in 2022, up from 15 in 2020. In total, 20 out of all 22 states that responded to this question in 2022 require the use of MFA. Overall, there was substantial growth from 2018 to 2020, and moderate growth from 2020 to 2022 in the adoption of MFA.

Figure 2: Multi-Factor Authentication Requirement: States that Responded in 2020 and 2022



Among the states that responded to this question in 2022, the most common type of MFA is a physical device (used in 13 states), followed by a time-based one-time password ("TOTP"), used in seven states, and then SMS authentication (used in six states). These three types of MFA were also the most common in 2020. Among the 18 states that responded to this question in both 2020 and 2022, one more reported using TOTP and three more reported using SMS authentication in 2022.

Figure 3: Types of Multi-Factor Authentication: States that Responded in 2022



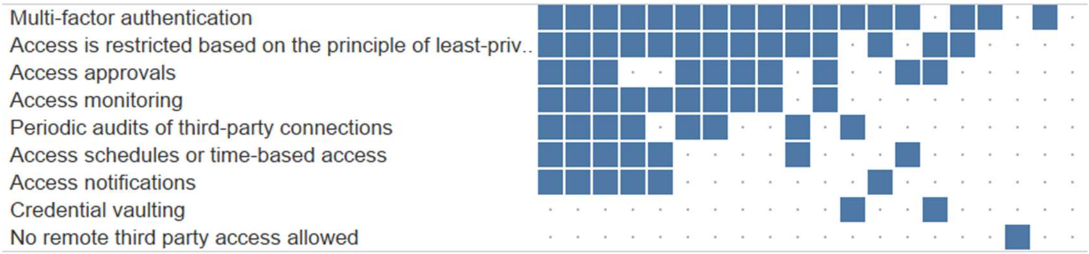
Third-Party Access

States must sometimes give third parties access to their VRDB system, including for critical security processes. When allowing third-party access, states employ a variety of measures

[14] Phishing and spear-phishing are common cyber threats 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. "Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks," Cybersecurity and Infrastructure Security Agency, October 22, 2009, updated August 25, 2020. https://www.cisa.gov/uscert/ncas/tips/ST04-014.

to manage risks. For the first time in 2022, CEIR's VRDB security survey asked states about their procedures for securing remote third-party VRDB access. Seventeen of the 20 states that responded to this question reported that they employ MFA for third-party access; 14 restrict access based on the principle of least privilege; 10 monitor access; 10 practice access approvals; eight conduct periodic audits of third-party connections; and seven employ time-based access.[15] One state indicated that it does not allow third-party access. It is encouraging that all 19 states that responded to this question have some measure of security in place for remote third-party VRDB access. Given this trend, we anticipate that going forward, states may adopt more of the security practices listed in Figure 4.

Figure 4: Practices for Securing Remote Third-Party Access: States that Responded in 2022



Ensuring System Integrity

Beyond securing access, states must have measures in place to maintain VRDB system integrity and prevent cyberattacks on an ongoing basis. To do this, VRDBs and connected systems must be designed to account for users' security shortcomings. While no one measure can ensure system 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.

Systems Audits

All systems that connect to the internet, including VRDBs, should be regularly audited to ensure security and functionality. This is another area of strength for the responding states.

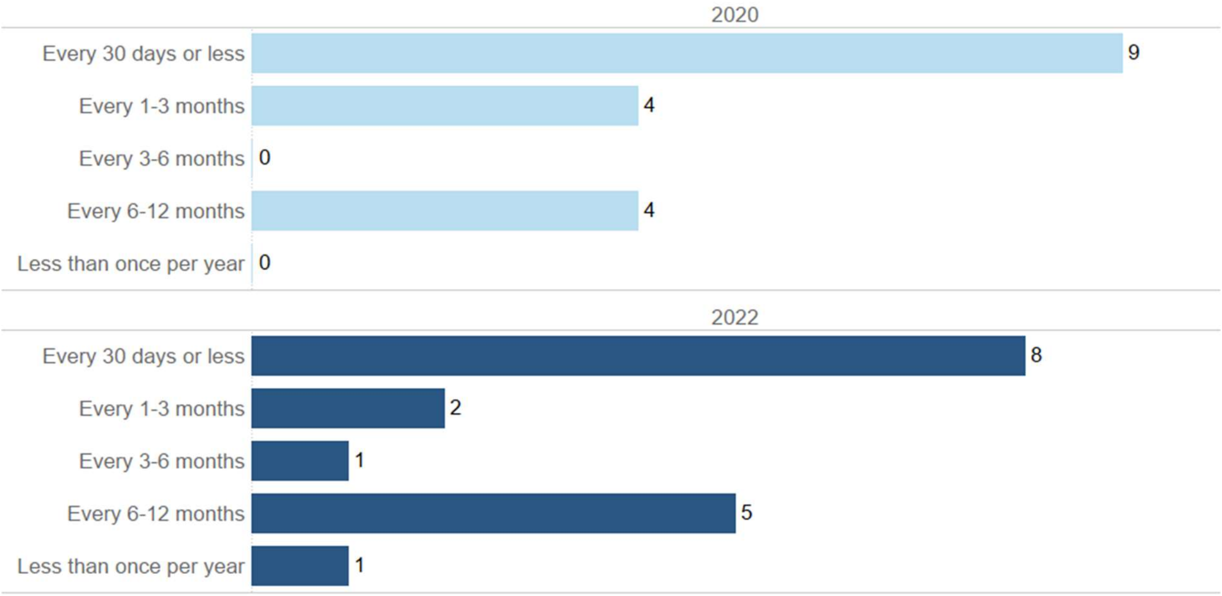
The 2022 survey found that, among the 22 states that responded to the question, 21 conduct systems audits and one does not. Among the states that responded to this question in both 2020 and 2022, all 18 reported conducting systems audits in the 2022 survey, up from 17 in 2020. This has long been common practice for states: all 19 states

[15] The principle of least privilege says that a subject should only be given the minimum rights necessary to complete its task. "Least Privilege," Cybersecurity and Infrastructure Security Agency, September 14, 2005, updated May 10, 2013. https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege.

that responded to this question in 2018 and 2020 indicated that they conduct systems audits.

The frequency with which states conduct systems audits varies. And while audit frequency matters, it is also the case that the need for frequent audits may differ depending on state-specific circumstances. For example, states with a large number of local election officials, and thus greater numbers of authorized VRDB users, may require more frequent audits than states that are much more centralized. Thus, variation in the frequency of systems audits is to be expected. Some states audit their systems at least monthly while others audit them less than once per year. Among states that responded in both 2020 and 2022, the frequency of systems audits appears similar.

Figure 5: Systems Audit Frequency: States that Responded in 2020 and 2022



IT Support

Experienced IT staff ordinarily handle the administration and maintenance of VRDBs and related systems. In 2022, 20 of 21 responding states reported having access to full-time IT support for their VRDB. Of these states, two reported having a contract with outside IT professionals and 18 reported receiving in-house support from at least one full-time staff member. The remaining state reported having a part-time IT staff member responsible for its VRDB. Among the 18 states that responded to this question in both 2020 and 2022, all but one reported having full-time IT support in both years and three shifted from contracting with outside professionals to in-house support in 2022.

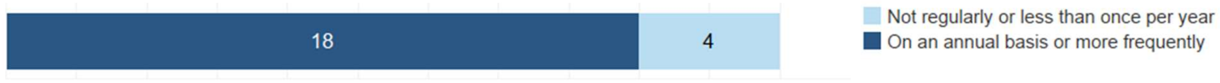
Training Users to Identify and Respond to Cyber Threats

Just as a system needs to be designed to prevent human error, users must be trained to minimize vulnerabilities. Even the most secure system may be compromised if a user shares their credentials or engages in other risky practices. As such, VRDB users must be trained to identify and respond to the kinds of cyber threats they might encounter. Through initiatives such as comprehensive user trainings and customized tabletop exercises, states are effectively managing many aspects of their VRDB user training and communication strategies.

User Training

In 2022, 22 out of 23 states reported that they train authorized VRDB users to identify cyber threats. Of these 22 states, 18 reported that they conduct cybersecurity training at least annually, an encouraging finding.

Figure 6: Cyber Threat Training Frequency: States that Responded in 2022

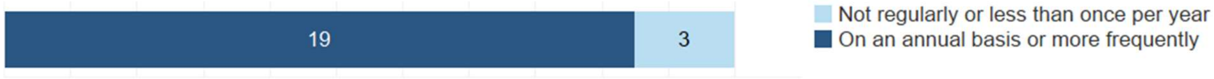


Phishing, a technique that can trick even the most careful users into handing over their login credentials, continues to be a prominent issue in cybersecurity.[16] After notable growth between 2018 and 2020, states continue to dedicate the necessary attention to this important issue in 2022. Among the 20 states that responded to both the 2018 and 2020 surveys, 17 reported training all VRDB users in 2018 while 19 reported training all users in 2020. All 19 states that responded to both the 2020 and 2022 surveys reported training all users to recognize phishing and spear-phishing. Additionally, all 23 respondent states reported that all users participate in training specifically to recognize phishing emails.

[16] CISA defines phishing as "a form of social engineering in which a cyber threat actor poses as a trustworthy colleague, acquaintance, or organization to lure a victim into providing sensitive information or network access. The lures can come in the form of an email, text message, or even a phone call. If successful, this technique could enable threat actors to gain initial access to a network and affect the targeted organization and related third parties. The result can be a data breach, data or service loss, identity fraud, malware infection, or ransomware." See CISA's infographic on phishing for more information: "Phishing," Cybersecurity and Infrastructure Security Agency, accessed January 20, 2023. https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf.

Frequency matters when it comes to training users on the threat of phishing.[17] In 2022, 19 out of 22 respondent states reported training VRDB users on phishing at least annually.

Figure 7: Phishing Training Frequency: States that Responded in 2022



Tabletop Exercises

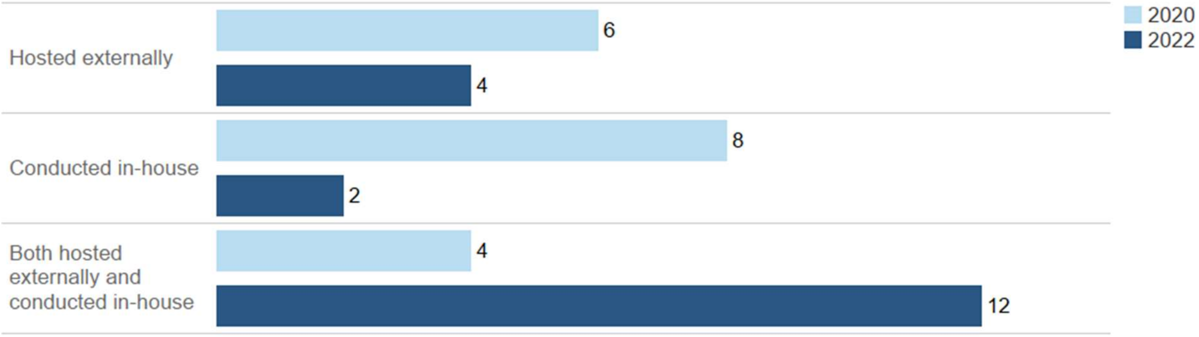
States often train election administrators using tabletop exercises (TTXs), which place participants in scenarios that simulate some of the worst scenarios that could occur during an election cycle.[18] Participants discuss the appropriate procedures to follow in a variety of circumstances and learn to act quickly in response to different crises.

Out of 23 respondent states in 2022, 22 reported using TTXs as part of their cybersecurity training. Fourteen reported participating in trainings hosted both externally and internally, six reported participating in external trainings only, and two reported participating only in internal trainings. Of the states that responded in both 2020 and 2022, all 19 reported conducting or attending tabletop exercises in both years. Among the 20 states that responded in 2018 and 2020, 12 reported using TTXs in 2018 and all 20 reported using TTXs in 2020. Once again, states demonstrate a pattern of substantial growth from 2018 to 2020 and maintenance of best practices between 2020 and 2022.

[17] At least one source specifies that phishing trainings should occur biannually, or every six months. See here for more information: Benjamin Reinheimer et al., "An investigation of phishing awareness and education over time: When and how to best remind users," USENIX, August 2020. https://www.usenix.org/conference/soups2020/presentation/reinheimer.

[18] "CISA and Election Security Partners Hold Tabletop the Vote Exercise in Preparation for 2022 Midterm Elections," Cybersecurity and Infrastructure Security Agency, August 19, 2022. https://www.cisa.gov/news/2022/08/19/cisa-and-election-security-partners-hold-tabletop-vote-exercise-preparation-2022; "CISA Tabletop Exercise Packages," Cybersecurity and Infrastructure Security Agency, accessed January 9, 2023. https://www.cisa.gov/cisa-tabletop-exercise-packages.

Figure 8: Tabletop Exercises: States that Responded in 2020 and 2022



Security Checkpoint: Tabletop Exercises

CISA offers a variety of free cybersecurity and physical security training exercises for election administrators. The exercises provide stakeholders an opportunity to analyze and improve security procedures to better respond to threats and attacks against election infrastructure.[I]

To provide election offices with tailored opportunities to analyze security threats and their response capabilities, CISA publishes customizable tabletop exercises for administrators to conduct their own exercises.[II] The agency's Tabletop Exercise Packages (CTEPs) for early voting and vote-by-mail both include a module with a hypothetical scenario in which the VRDB is breached.[III] The exercises cover discussion questions specific to the scenario and contain an appendix of resources, references, and broadly applicable discussion topics, including public affairs concerns and legal considerations.

In addition to CTEPs, CISA conducts an annual "Tabletop the Vote" (TTV) exercise in coordination with the U.S. Election Assistance Commission, National Association of Secretaries of State, and National Association of State Election Directors.[IV] Public and private stakeholders meet over the course of a few days to address hypothetical scenarios affecting elections operations.

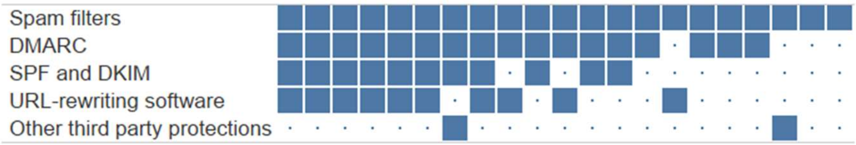
Using these exercises as a "practice round" before elections take place helps administrators prevent VRDB breaches by identifying security shortcomings early on and improving responsiveness to threats and attacks.

[I] "Election Security Training and Exercise Offerings," Cybersecurity and Infrastructure Security Agency, September 2022. https://www.cisa.gov/sites/default/files/publications/election-security-training-exercises-flyer_508.pdf.
[II] CISA, "Election Security Training."
[III] "Early Voting CTEP Situation Manual," Cybersecurity and Infrastructure Security Agency, updated October 2022. https://www.cisa.gov/sites/default/files/publications/Early-Voting-CTEP-Situation-Manual-508-20221031-v00_0_0.docx; "Elections Vote By Mail CTEP Situation Manual," Cybersecurity and Infrastructure Security Agency, updated October 2022. https://www.cisa.gov/sites/default/files/publications/Elections-Vote-by-Mail-CTEP-Situation-Manual-2021-508-20221031-v00.docx.
[IV] CISA, "Tabletop the Vote Exercise."

Implementing Email Security Protocols

Email protections help prevent phishing attempts and block harmful email attachments that could lead to a VRDB being compromised. These protections usually verify a sender or check the contents of a message. In 2020 and 2022, all responding states had at least one form of email protection in place. In both years, all but one state reported using spam filters, many in combination with other email protections. Among these other protections, DMARC and SPF and DKIM, were the most common selections. [19,20] Since 2020, there has been a noticeable increase in the proportion of respondent states utilizing DMARC and URL-rewriting software. This is a continuation of the noted improvement between 2018 and 2020. Specifically, states that responded to the question in both those years showed growth in the use of DMARC as well as SPF and DKIM.

Figure 9: Email Protections: States that Responded in 2022



[19] 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 weaknesses in SPF and DKIM. "About SPF, DKIM, and DMARC for Email Authentication," Knowledge Base, July 21, 2021. https://kb.iu.edu/d/azlu; "Overview," DMARC, accessed January 9, 2023. https://dmarc.org/overview/.

[20] 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 on URL-rewriting software, see for example Microsoft's ATP Safe Links: Office 365. "Set up Safe Links policies in Microsoft Defender for Office 365," Microsoft, December 14, 2022. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure?view=o365-worldwide.

Detection

No matter how many preventative measures are in place, no system is impervious to attack. It is therefore vital that states are able to detect and respond to threats as they appear. To do this, states monitor and audit their VRDB activity on an ongoing basis using tools like network monitoring systems. On the whole, states report many efforts in line with best practices for monitoring and auditing their VRDBs. However, there continues to be room for improvement in this domain of VRDB security.

Monitoring and Auditing VRDB Activity

Monitoring the nature and type of VRDB activity is important. Below, we detail how states examine login attempts, inputs, and overall VRDB traffic to look for signs of problematic trends or incidents.

Login Attempts

Monitoring and auditing attempts to log in to a VRDB—whether the login attempts are successful or not—is an important measure to help detect malicious activity.[21] In 2022, 19 of 21 responding states reported monitoring and auditing login attempts, with 16 of these states reporting that they monitor and audit both successful and failed login attempts and three reporting that they do so only for failed login attempts. In 2018, 15 of 26 responding states reported monitoring both successful and unsuccessful attempts, five reported monitoring only failed attempts, and six indicated that they did not monitor or audit any attempts. In 2020, 26 out of 28 responding states reported monitoring login attempts and 24 reported monitoring both successful and failed attempts. The growth in monitoring and auditing VRDB login attempts from 2018 to 2020 appears to have been sustained from 2020 to 2022.

However, it is worth noting that of the 18 states that responded in 2020 and 2022, two fewer states reported monitoring and auditing both successful and failed login attempts in 2022 than in 2020 (15 and 17, respectively). While this represents mild regression among this subset of states and may warrant attention in future surveys, the overall prevalence of monitoring and auditing login attempts is encouraging.

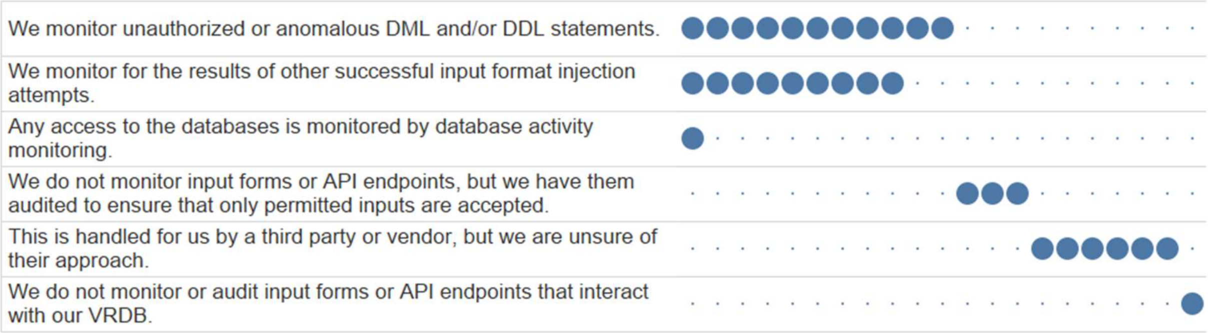
Malicious Inputs

In addition to threats via login attempts, malicious actors may also threaten VRDBs by attempting to inject database commands or other code to alter the system or obtain administrative access to the backend. Of 21 responding states in 2022, 11 indicated that

[21] 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.

they monitor for unauthorized or abnormal database queries or improperly formatted inputs. Of the remaining states, three indicated that they audit their input forms and API endpoints to ensure that only permitted inputs are accepted; six responded that a third party or vendor handles any such monitoring and that they are unsure of that third party's approach; and one indicated that such monitoring is not a factor in their threat detection apparatus.

Figure 10: Practices for Protecting Against Malicious Input: States that Responded in 2022



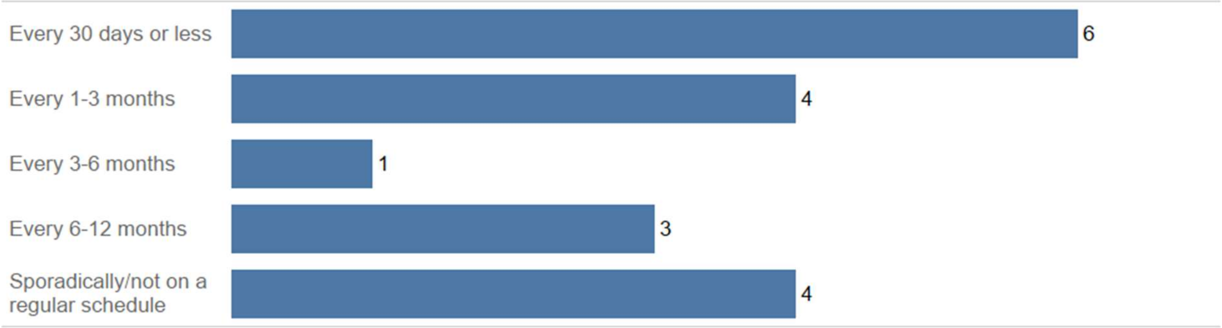
VRDB Traffic

Another aspect of VRDB activity that states monitor involves changes in traffic over time. It is important to know when VRDB activity deviates from past trends in order to investigate the source of the change. An increase in VRDB traffic is usually innocuous, like when a voter registration drive registers many people at once. However, in rare cases an increase in traffic may be the result of bad actors. Additionally, changes to high-profile records, such as those of celebrities, can provide an early warning sign of VRDB tampering. In 2022, 18 of 21 responding states reported conducting regular audits to better understand the traffic to their VRDB, such as by analyzing traffic volume, origin, and type of activity. Among the 18 states that responded in 2020 and 2022, 18 reported conducting such audits in 2020 and 16 reported doing so in 2022.[22]

As in 2020, the frequency of VRDB traffic audits varies considerably among the 21 states that responded to this question in 2022. The most common response was "Every 30 days or less," but several states reported auditing traffic less frequently, with a significant portion reporting that audits happen sporadically or not on a regular schedule. The frequency of VRDB traffic audits remains an area where states can improve.

[22] One reason for this decrease may concern third-party oversight. For example, one state that reported auditing VRDB traffic in 2020 but not in 2022 indicated that it has since partnered with a third party to implement IP address restrictions limiting access to its VRDB. Because of the new restrictions, this state stopped conducting traffic audits.

Figure 11: Traffic Audit Frequency: States that Responded in 2022



In 2022, states were also asked whether they monitor additional indicators of malfeasance and were given an opportunity to write in answers. Thirteen reported monitoring the total volume of VRDB traffic over time in comparison with expected traffic; two reported monitoring high-profile records for unexpected changes; and one reported instructing local election officials on how to monitor records for indicators of attempted malfeasance.

Network Monitoring Systems

Network monitoring systems are a common tool used to detect threats to a VRDB. These systems constantly monitor external network traffic to affirmatively prevent VRDB intrusions or alert IT staff about suspicious activity. Of the 21 responding states in 2022, 18 indicated that they use a system that automatically alerts them to irregular VRDB activity. Among the 18 states that responded in both 2020 and 2022, 16 reported that they use such a system in 2022, down from 18 in 2020.

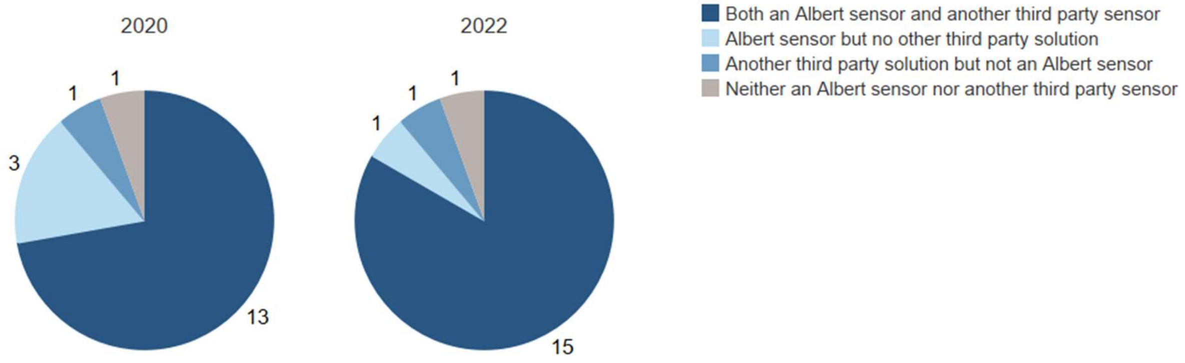
Albert network monitoring is a network monitoring solution that is offered exclusively to U.S. state, local, tribal, and territorial governments and works by pairing an intrusion detection system with real-time expert threat analysis.[23] Among 21 responding states, 19 reported using one or more Albert sensors to monitor their VRDB traffic in 2022. Of the 18 states that responded to this question in both 2020 and 2022, 16 reported that they use Albert sensors as part of their threat detection apparatus in both years. While the practice is common now, there was substantial growth in the use of Albert sensors between 2018 and 2020: among the 20 states for which we tracked progress between these years, six more states used Albert sensors in 2020 than in 2018.

Beyond Albert, states can use a wide variety of other third-party solutions to monitor their VRDBs: 14 states reported using a third-party network monitoring solution since 2020, and

[23] "Albert Network Monitoring," Center for Internet Security, accessed January 9, 2023. https://www.cisecurity.org/services/albert-network-monitoring/.

16 reported using one in 2022. Overall, in 2022, 19 of the 21 responding states indicated that they use another third-party network monitoring solution with their VRDB.

Figure 12: Albert Sensor and Other Third-Party Solution Use: States that Responded in 2020 and 2022



Security Checkpoint: Albert Sensors

Albert is a type of Intrusion Detection System (IDS) built for and utilized exclusively by State, Local, Tribal, and Territorial (SLTT) networks.[I] Albert sensors are operated by the Center for Internet Security and often developed and deployed with funding from CISA.[II]

Albert passively monitors network traffic data to identify and report malicious activity. If Albert identifies a signature match to a known security threat, it escalates the threat to a 24/7/365 security operations center operated by the Multi-State Information Sharing and Analysis Center (MS-ISAC). There, analysts review alerts, dismiss false positives, and report actionable threats—typically within six minutes after detection.[III] According to the Center for Internet Security, Albert should be used as part of a "layered 'defense in depth' approach" to provide the most effective protection.[IV]

SLTT organizations may not have the capacity to comprehensively monitor VRDB network activity and Albert can help fill the gap.[V] The sensors also provide a more complete view of the national election security landscape, with over 800 deployed as of early 2022.[VI]

[I] "About the Albert Sensor," Center for Internet Security, February 23, 2022. https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2022/2022-02-23-facts-about-albert-sensor---final.pdf
[II] CIS, "About the Albert Sensor."
[III] CIS, "Albert Network Monitoring."
[IV] CIS, "About the Albert Sensor."
[V] CIS, "Albert Network Monitoring."
[VI] CIS, "About the Albert Sensor."

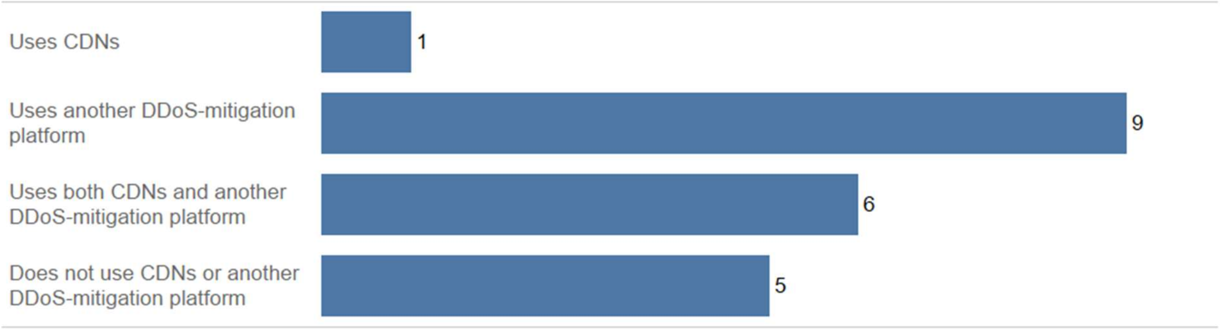
Mitigation

If a cyberattack is detected, states must be ready to respond swiftly. Some resources, such as content delivery networks (CDNs) (sometimes referred to as content distribution networks) 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.[24] Other practices, such as regularly backing up systems and using paper pollbooks, serve as part of contingency plans to restore systems to a reliable state and otherwise mitigate the effects of any successful attack on a VRDB.

CDNs and DDoS Mitigation Tools

DDoS attacks are a common way for malicious actors to disrupt legitimate users' access to a website or other networked computer system.[25] CDNs and DDoS mitigation tools can address these and other similar attacks. In practice, both CDNs and DDoS mitigation tools can be effective ways to ensure networked systems stay online and usable. Among the 21 responding states in 2022, 15 indicate that they use DDoS mitigation tools and seven report making use of CDNs. Six of the states using CDNs indicated that their CDN is geofenced to prevent data from leaving the U.S.

Figure 13: CDNs and DDoS-Mitigation Platforms: States that Responded in 2022



[24] 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.

[25] DDoS attacks work by leveraging various sources of traffic to overwhelm the resources of a target. "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," Cybersecurity and Infrastructure Security Agency, November 4, 2009, updated October 28, 2022. https://us-cert.cisa.gov/ncas/tips/ST04-015.

Security Checkpoint: CDNs & DDoS Mitigation Tools

Distributed denial-of-service (DDoS) attacks leverage multiple sources of traffic to overwhelm a targeted system and cause service outages.[I] While they represent a threat in and of themselves, DDoS attacks are also sometimes used as a diversion tactic to blind system users and administrators to other malicious activity.[II] By limiting their vulnerability to such attacks, organizations using CDNs and other DDoS mitigation tools can more readily detect any other potentially malicious activity that a DDoS attack may be trying to obscure.

Content delivery networks (CDNs) are geographically distributed servers that connect from the origin server to the server closest to the end-user for enhanced speed, reduced latency, and secure network activity.[III] CDNs redundantly maintain content over several servers by storing a cached or "copied" form of the original server—useful for distributing bandwidth in case a single server is overwhelmed or otherwise compromised.[IV] Additionally, some CDN providers also include dedicated distributed denial-of-service (DDoS) protection packages, which is why CDNs are often discussed alongside other DDoS mitigation tools.[V]

Broadly, CDNs reroute network traffic through cached servers to prevent excessive network traffic from slowing down or otherwise affecting the original server.[VI] In the case of a DDoS attack on a VRDB, CDNs can mitigate the extra traffic intended to overwhelm the network to avoid network failures and help authorized users maintain access to the database.[VII]

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, when unusual traffic is detected which deviates from this baseline, it can be harmlessly redirected before it reaches its destination.[VIII] This keeps a protected system from being overwhelmed, preserving user access and maintaining operational capabilities.

[I] "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," Cybersecurity and Infrastructure Security Agency, November 4, 2009, updated October 28, 2022. https://us-cert.cisa.gov/ncas/tips/ST04-015.

[II] CISA, "Understanding and Responding to DDoS Attacks," 4.

[III] Ben Lutkevich, "CDN (Content Delivery Network)," TechTarget, last updated October 2021. https://www.techtarget.com/searchnetworking/definition/CDN-content-delivery-network.

[IV] "What is a CDN? How do CDNs work?" Cloudflare, accessed January 9, 2023. https://www.cloudflare.com/learning/cdn/what-is-a-cdn/.

[V] "Can a CDN Really Protect You Against DDoS Attacks?" Insights for Professionals, February 2, 2021. https://www.insightsforprofessionals.com/it/security/can-cdn-protect-you-against-ddos-attacks.

[VI] IFP, "Can a CDN Protect Against DDoS Attacks?"

[VII] "Content Delivery Network Security — Increased Security Against DDoS Attacks with CDN Solutions," Beluga CDN, accessed January 9, 2023. https://www.belugacdn.com/content-delivery-network-security/; "Understanding and Responding to Distributed Denial-of-Service Attacks," Cybersecurity and Infrastructure Security Agency, October 28, 2022. https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf.

[VIII] "Security Tip (ST04-015): Understanding Denial-of-Service Attacks."

Contingency Plans

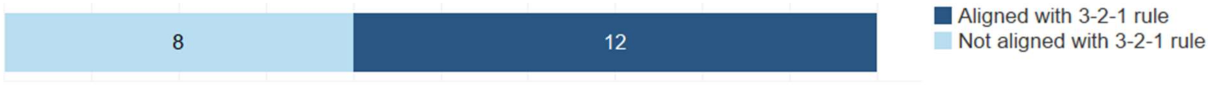
If all else fails and an attack successfully alters or impedes a VRDB, there must be a plan to both restore the system and, in the meantime, ensure elections continue to be administered properly. Contingency plans around backups and pollbooks can protect against serious interruptions to the administration of elections.

Backups

Creating regular VRDB backups is the best insurance against the permanent loss of voter data. All 21 states that responded to the question in 2022 indicated that they regularly back up their VRDB, with 20 reporting that they do so daily or more frequently, and one reporting that it does so every two to seven days. Among the 18 states that responded in 2020 and 2022, 16 reported backing up their VRDB daily or more frequently in 2020 and 17 reported doing so in 2022.

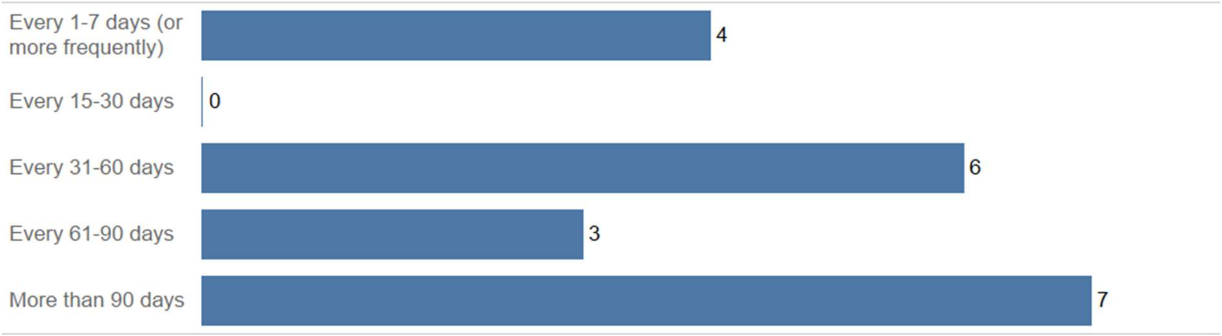
For the first time, our VRDB survey asked states if they follow the 3-2-1 rule (see below) for storing backups. Of the 20 states that responded to this question, 12 reported that their storage practices for backups follow the rule, representing a solid foundation but a possible area for improvement in VRDB security across the states.

Figure 14: Alignment with the 3-2-1 Rule in Backing Up the VRDB: States that Responded in 2022



All 21 responding states also indicated that they test their VRDB backups to ensure they work. As in past years, testing frequency varies significantly, ranging from at least once per week to less than once every 90 days, with most states indicating that they conduct these tests every one to three months.

Figure 15: Frequency of Testing VRDB Backups: States that Responded in 2022



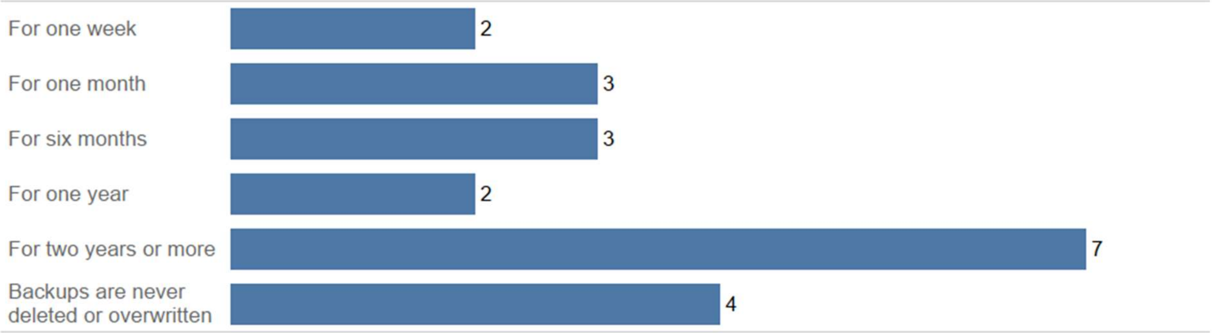
Security Checkpoint: The 3-2-1 Backup Rule

Secure backups are an essential component of any cybersecurity mitigation plan, as they allow administrators to quickly restore a system and preserve unmodified data in the event of a cybersecurity attack.[I] As best practice, cybersecurity experts advise that such backups follow the 3-2-1 rule: administrators should keep *three* copies of backup data stored on at least *two* different kinds of media, with at least *one* backup kept off-site. This redundant structure helps insulate backups from the effects of an attack, so that even if malicious actors manage to compromise the main system or alter data stored in one medium, election officials can quickly restore the VRDB to a known reliable state using another backup. Of course, election officials should test these backups frequently to ensure that all necessary or critical information is being captured, that staff know how to recover data from backups to ensure continuity of operations in the event of an attack, and that the entire process works as intended.[II]

[I] "Best Practices for Election Technology," U.S. Election Assistance Commission, June 2022, 6. https://www.eac.gov/sites/default/files/electionofficials/security/Best_Practices_for_Election_Technology_508.pdf.
[II] EAC, "Best Practices."; "Security Tip (ST16-001): Securing Voter Registration Data," Cybersecurity and Infrastructure Security Agency, February 1, 2021. https://www.cisa.gov/tips/st16-001.

States also vary with respect to the amount of time for which these backups are preserved before being deleted or overwritten, ranging from one week to indefinitely, with most states indicating that they preserve backups for at least one year.

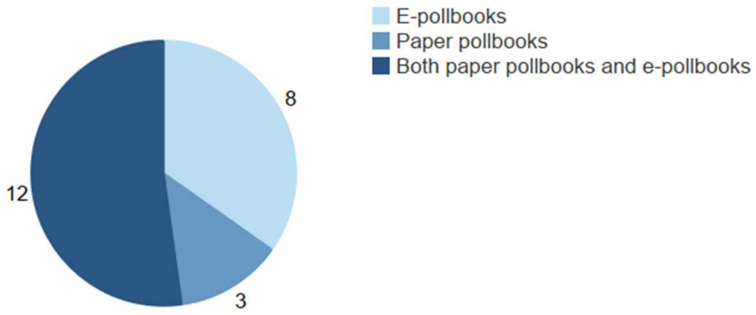
Figure 16: Preservation of VRDB Backups: States that Responded in 2022



Pollbooks

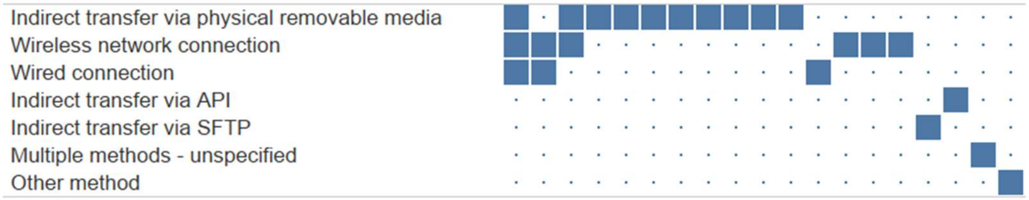
States can prepare for a possible Election Day attack on their VRDB by using pollbook backups and provisional ballots. Mitigation techniques vary based on the types of pollbooks states use, and states sometimes use multiple types of pollbooks for a given election. Of the 23 states that responded to the 2022 survey, 12 reported using a mix of paper pollbooks and electronic pollbooks (e-pollbooks) to check in voters, with eight others using primarily e-pollbooks, and three relying solely on paper pollbooks.

Figure 17: Use of E-Pollbooks and Paper Pollbooks: States that Responded in 2022



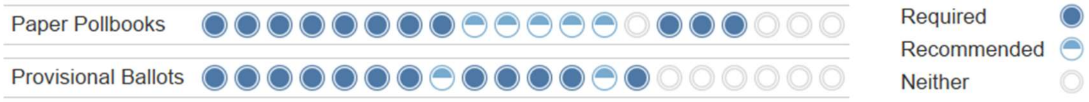
The 20 states that reported using e-pollbooks to some extent use a variety of methods to securely connect to their VRDB to load or transmit voter registration data, with the most common method by far being indirect transfers by physical removable media, such as USB sticks. Several states also make use of secure wired and wireless connections to transfer data.

Figure 18: How E-Pollbooks Connect to the VRDB: States that Responded in 2022



All 20 states that reported using e-pollbooks also reported having at least one type of contingency plan in place should their e-pollbooks fail. Contingency plans may include having paper copies of the pollbook on hand at polling places, maintaining a sufficient number of provisional ballots, or any number of other preventative measures. Most responding states require that local election officials keep a paper pollbook as backup, provide provisional ballots to voters if e-pollbooks fail, or both, with many that do not require one of these practices still advising local officials to implement them.

Figure 19: Backup Practices for E-Pollbooks: States that Responded in 2022



Conclusion

The 2022 survey is the third that CEIR has conducted to assess VRDB security across the states. Since the inaugural survey in 2018, states have demonstrated a commitment to best practices in VRDB security. Our reports on state responses to these surveys identify specific areas of strength and opportunities for growth.

As of 2022, states have largely maintained their alignment with the best practices in prevention, detection, and mitigation that they demonstrated in previous years, sustaining the progress made between 2018 and 2020. Furthermore, MFA requirements are now widespread, representing progress in an area that the 2020 report identified for growth. The 2020 report called for some improvement in monitoring and auditing VRDB traffic and login attempts, and that improvement remains a work-in-progress. This year's report also notes some regression in the number of responding states that require passwords to be at least eight characters long. In both areas, we would expect progress over the next two years. Nonetheless, the overwhelming majority of the evidence in this report indicates that the state of VRDB security is strong.

In response to insight from experts in the field, the 2022 survey introduced new questions. For the first time, CEIR's survey asked states about the security of remote third-party access and adherence to the 3-2-1 rule when backing up VRDBs. It also asked more detailed questions about e-pollbooks. Future VRDB surveys will continue to keep pace with developments in the field of cybersecurity. CEIR will also seek to increase survey response rates to provide information from more states and shed further light on broad trends in future reports.

At a time when election administrators are plagued by rampant misinformation and subject to intense pressure, it is crucial that elections are successful and secure. The strength and resilience of VRDBs in the U.S. underscores the integrity of our elections and should bolster voter trust and confidence. As always, threats will continue to evolve, requiring that state responses and the best practices they employ stay ahead of them. For this reason, CEIR will continue its research in this critical field.

Appendix A: Survey Instrument

i. Name
ii. Title
iii. State
iv. Email address

(As a reminder, we will keep state-specific responses confidential to maintain security. Results will be aggregated.)

1. Are users required to use multi-factor authentication when accessing your statewide voter registration database (VRDB) system?
    a. Yes
    b. No

IF YES: What forms of authentication do users use in addition to a password? (Select all that apply.)

a. A physical device like a security token, smartcard, grid card, or security key (yubikey or Feitian device)
b. Personal biometric data, like a fingerprint
c. SMS authentication
d. A secondary Time-Based One-Time Password (TOTP) (often provided by mobile phone apps, e.g., Google Authenticator)
e. Other: (Please specify.) _______________

2. What requirements are in place for user passwords? (Select all that apply.)
    a. Minimum number of characters required
    b. Must use at least one uppercase letter
    c. Must use at least one lowercase letter
    d. Must use at least one number
    e. Must use at least one special character
    f. Cannot match a previously used password
    g. Cannot match commonly used passwords (e.g., “password1234”)
    h. Cannot match user’s information (e.g., user’s last name, birthday)
    i. Must use randomly generated passwords
    j. Cannot use more than a certain number of characters
    k. Must use a passphrase (e.g., combining multiple words into a long string)
    l. Password not required because users use two other factors
    m. Other: (Please specify.) _______________
    n. None of these

IF MINIMUM NUMBER OF CHARACTERS (A): What is the minimum number of characters required?

[Enter a numeric number.]

3. Are users required or permitted to use a password manager?
    a. Required
    b. Permitted
    c. Neither

4. Are users required to change their password(s)?
    a. Yes
    b. No

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

   a. Every 30 days or fewer
   b. Every 1-3 months
   c. Every 3-6 months
   d. Every 6-12 months
   e. Less frequently than once per year

5. What practices are in place for securing *remote third-party access* to the VRDB? (Select all that apply)
    a. Access is restricted based on the principle of least-privilege (i.e., user access is limited to the resources required to perform set tasks)
    b. Periodic audits of third-party connections
    c. Multi-factor authentication
    d. Credential vaulting
    e. Access notifications
    f. Access schedules or time-based access
    g. Access approvals
    h. Access monitoring
    i. Other: (Please specify.) _______________

6. How are your email servers hosted?
    a. Our agency hosts our own email servers
    b. Another state agency hosts our email servers
    c. Our email servers are hosted in the cloud
    d. Other: (Please specify.) ________________

7. What types of email protection do you have in place? (Select all that apply.)
    a. Spam filters
    b. URL-rewriting software (e.g., Proofpoint)
    c. SPF and DKIM
    d. DMARC
    e. None of these
    f. Other: (Please specify.) _______________

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

[Please specify.]

8. Does your office have at least one designated IT staff member who is responsible for your statewide VRDB?
   a. Yes, we have a full-time IT staff member responsible for our VRDB.
   b. Yes, we have a part-time IT staff member responsible for our VRDB.
   c. No, but we contract with an outside party for full-time IT support for our VRDB.
   d. No, but we contract with an outside party for part-time IT support for our VRDB.
   e. No, we do not have skilled IT support for our VRDB.

9. Do you conduct systems audits to identify possible security vulnerabilities?
   a. Yes
   b. No

IF YES: How frequently do you conduct systems audits?

   a. Every 30 days or less
   b. Every 1-3 months
   c. Every 3-6 months
   d. Every 6-12 months
   e. Less than once per year
   f. Sporadically but not on a regular schedule (e.g., after a cyber incident)

10. Are authorized users trained on how to identify cyber threats?
   a. Yes
   b. No

IF YES: How frequently does this training occur?

   a. At least annually
   b. Not regularly or less than once per year

11. Do you engage in training specifically about phishing and spear-phishing?
   a. Yes
   b. No

IF YES: How frequently does this training occur?

   a. At least annually
   b. Not regularly or less than once per year

IF YES to Q11: Who participates in this training?

   a. All users are trained to recognize phishing emails
   b. Only certain users are trained to recognize phishing emails

12. Do you conduct or attend tabletop exercises (TTX) for cybersecurity training?
    a. Yes
    b. No

IF YES: Who participates in these exercises?

   a. All users
   b. Only some users

IF YES to Q12: Are these exercises conducted in-house or hosted externally?

   a. Conducted in-house
   b. Hosted externally
   c. Both

13. Does your office (or a third party) monitor and audit login attempts to your VRDB?
    a. Yes, we monitor and audit *both successful and failed* login attempts.
    b. Yes, we monitor and audit *only failed* login attempts.
    c. No, we do not monitor login attempts.
    d. This is handled for us by a third party or vendor, but we are unsure of their approach.

14. Which of the following practices, if any, does your office (or a third party) use to monitor your VRDB for malicious input? (Select all that apply.)
    a. We monitor unauthorized or anomalous data manipulation language (DML) statements and/or data definition language (DDL) statements.
    b. We monitor for the results of other successful input format injection attempts.
    c. We do not monitor input forms or Application Programming Interface (API) endpoints, but we have audited all of our input forms and API endpoints to ensure that only permitted inputs are accepted.
    d. We do not monitor or audit input forms or API endpoints that interact with our VRDB.
    e. This is handled for us by a third party or vendor, but we are unsure of their approach.
    f. Other: (Please specify.) ________________

15. Does your office (or a third party) monitor any of the following additional indicators of attempted malfeasance?

a. Yes, we monitor the volume of VRDB traffic over time compared to expected traffic.
b. Yes, we monitor high-profile records (e.g., voter registration records of celebrities or other public figures) for unexpected changes.
c. Yes, we monitor some other indicator of attempted malfeasance: (Please specify.) ________________
d. No, we do not monitor any other indicators of attempted malfeasance.
e. This is handled for us by a third party or vendor, but we are unsure of their approach.

16. Does your office use content distribution networks (CDNs) or DDoS-mitigation platforms (e.g., Cloudflare's Athenian Project or Google's Project Shield) for your VRDB? (Select all that apply.)
    a. Yes, we use CDNs.
    b. Yes, we use a DDoS-mitigation platform.
    c. No, we do not use either of these.

IF "YES, WE USE CDNS" (A): Is the CDN you use geofenced so that it cannot send data outside the U.S.?

a. Yes
b. No
c. Unsure

17. Do you conduct regular audits to better understand the traffic to your VRDB, such as analyzing traffic volume, origin, type of activity, etc.?
    a. Yes
    b. No

IF YES: How frequently do you conduct VRDB traffic audits?

a. Every 30 days or less
b. Every 1-3 months
c. Every 3-6 months
d. Every 6-12 months
e. Less than once per year
f. Sporadically/not on a regular schedule (e.g., only after a cyber security incident)

18. Is there a system in place that automatically alerts your office if irregular VRDB activity (e.g., database injection attempts, unusual VRDB traffic, high number of failed login attempts, etc.) is detected?
    a. Yes, we are automatically alerted about irregular activity.
    b. No, we are not automatically alerted about irregular activity.

19. Do you use one or more Albert sensors to monitor your VRDB?
    a. Yes
    b. No

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

21. Do you back up your VRDB and related systems?
    a. Yes
    b. No

IF NO, SKIP TO Q26

IF YES: How frequently do you back up your VRDB and related systems?

a. Daily (or more frequently)
b. Every 2-7 days
c. Every 8-14 days
d. Every 15-30 days
e. Every 31-60 days
f. Every 61-90 days
g. More than every 90 days

22. How long are backups preserved before being deleted or overwritten?
    a. For one day
    b. For one week
    c. For one month
    d. For 6 months
    e. For one year
    f. For 2 years or more
    g. Backups are never deleted or overwritten.

23. Do you store a backup offline?
    a. Yes
    b. No

24. Do your backup storage practices align with the 3-2-1 rule (i.e., three copies on two different media, with one copy kept offsite)?
    a. Yes
    b. No

25. Do you test your VRDB backups to ensure they work?
    a. Yes
    b. No

IF YES: How frequently do you test your VRDB backups?

a. Every 1-7 days (or more frequently)
b. Every 8-14 days
c. Every 15-30 days
d. Every 31-60 days
e. Every 61-90 days
f. More than 90 days

26. What system is used to check in voters in your state?
    a. Paper pollbooks
    b. Electronic pollbooks (e-pollbooks)
    c. Our state uses a mix of both paper pollbooks and e-pollbooks.

IF EPOLLBOOKS (B) or BOTH (C):

27. How do your e-pollbooks connect to the VRDB to load or transmit voter registration data? (Select all that apply.)
    a. Wireless network connection
    b. Wired connection
    c. Indirect transfer via physical removable media (e.g., a USB stick)
    d. Other: (Please specify.) ________________

The next few questions ask about the contingencies in place in case the e-pollbook fails during early voting or on Election Day (due to compromise, hardware failure, etc.).

28. Please select the statement that most accurately reflects your policies and procedures.
    a. Our state *requires* local election officials to keep a paper pollbook as backup.
    b. Our state *advises* local election officials to keep a paper pollbook as backup.
    c. Neither

28. Please select the statement that most accurately reflects your policies and procedures.
    a. Our state *requires* local election officials to have on hand or be able to produce provisional ballots in case the e-pollbook fails during early voting or on Election Day.
    b. Our state *advises* local election officials to have on hand or be able to produce provisional ballots in case the e-pollbook fails during early voting or on Election Day

    c. Neither

29. IF YES, REQUIRES OR ADVISES: Does your state specify how many provisional ballots it requires or advises local election officials to have on hand or be able to produce if an e-pollbook fails?
    a. Yes, our state requires or advises local election officials to have on hand or be able to produce *a specific number of ballots*
    b. Yes, our state requires or advises local election officials to *follow a rule or calculation* to determine how many provisional ballots to have on hand or be able to produce
    c. No

30. IF YES (either A or B): Please provide that specific number or describe the rule or calculation below.
    a. FREE RESPONSE

31. If you have other contingencies in place, please briefly describe them below.

[Free Response]

32. Has your state made any other changes or implemented new solutions in cybersecurity since 2020 that were not mentioned above? Please highlight these changes here:

[Free response.]