



Recognizing and Addressing Threats to Statewide Voter Registration Databases

July, 2026



EXECUTIVE SUMMARY

Recently declassified records revealed that China breached multiple state voter registration systems prior to the 2020 election. Unfortunately, this is not a new phenomenon. Unclassified reports from the last decade reveal that Statewide Voter Registration Databases (VRDB) are attractive targets for foreign adversaries.¹ Hackers have attempted to breach voter registration systems in all 50 states, with confirmed successes in at least 20 states. However, experts have routinely minimized the significance of successful voter registration breaches and the exposure of sensitive personal data used for voter verification. This failure to identify and accurately describe the potential threats makes U.S. elections less secure.

State and local election officials must prioritize enhanced defenses to protect voter registration databases, and to limit the ways that compromised data can be exploited. Steps should be taken to prevent bad actors from using stolen data to successfully obtain absentee ballots, alter voter registration information, or add and delete registrants. Implementing and maintaining safeguards is essential to protecting the electoral process and sustaining public confidence in elections.

It is imperative to be realistic about the threats posed by foreign adversaries to our critical systems, including election infrastructure. Accurately assessing and communicating the potential for serious consequences is fundamental to effective preparedness and risk management. While candid acknowledgment of these threats may cause concern, it enables critical infrastructure owners to make informed decisions about security measures and mitigation strategies, thereby reducing vulnerability to worst case scenarios. Ignoring or minimizing risks undermines the ability to implement robust controls and leaves critical systems exposed. Transparent recognition of the threat landscape is essential for developing resilient defenses and ensuring the integrity and security of our election systems.

This product provides an unclassified overview of the threats to statewide voter registration databases from both foreign and domestic actors. It relies on reporting from the intelligence community, law enforcement, and state election officials. This report is intended to inform state and local election officials of the associated threats and the need to implement recommended mitigating controls.

HISTORY OF VOTER REGISTRATION SYSTEM BREACHES

Below are examples of unclassified reports of breaches of voter registration databases in the last ten years.

- Russian government cyber actors attempted to identify and exploit SQL database vulnerabilities in web servers and databases. The FBI reported that they lacked insight into the extent to which the attempts were successful. However, in at least two separate instances, Russian actors accessed voter registration files from a US county website.² (June 2016)
- The District Attorney in Riverside County, California revealed that a bad actor used the state's voter registration website to change the party affiliation of a large number of registered voters. The individual made the changes by leveraging access to voters' personal information (name, date of birth, driver's license, or Social Security number) to make the change without the voters' knowledge or consent.³ (July 2016)
- Russian actors hacked the website of a state board of elections and stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers.⁴ (July 2016)
- Russian actors hacked into the computers of a U.S. vendor that supplied software used to verify voter registration information.⁵ (August 2016)
- DHS and FBI confirmed that Russian actors conducted election system reconnaissance to identify vulnerable databases, usernames, and passwords in webpages of state and local governments and probed voter registration database in **all 50 states**. They could not confirm how many of the probes resulted in successful breaches.⁶ In January 2017, WH officials reported that the federal assessment was that networks in at least seven states were compromised.⁷ (2016)
- Arizona experienced a breach and the Illinois State Board of Elections announced that attackers gained access to voter registration data, including names, addresses, birth dates, and partial Social Security numbers.⁸ (2016)
- Kennesaw State University, which was responsible for supporting Georgia's voter registration database, was found to expose nearly 7 million voter records including driver's license and Social Security numbers of registered voters. The data may have been exposed for as long as seven months.⁹ (March 2017)

- Chinese state-sponsored cyber actors aggressively targeted U.S. critical infrastructure to steal sensitive data and personally identifiable information (PII).¹⁰ (August 2021)
- CISA and the FBI reported that members of the Iranian Republic Guard Corp attempted to exploit websites to obtain voter registration data. They confirm that the actor successfully obtained voter registration data in at least one state. They could not determine if the attempts were successful in the other 11 states targeted.¹¹ (September 2020)
- Pro-Russian hackers claimed to have conducted a Distributed Denial of Service (DDoS) attack that resulted in temporarily restricted access to a public-facing US state election office website.¹² (2022)
- Suspected Chinese cyber actors scanned both election-related and non-election state government websites. Other suspected PRC cyber actors also collected publicly available U.S. voter information.¹³ (2022)
- New Hampshire election officials discovered that a vendor selected to replace the state's aging voter registration database had offshored part of the project. The software had been configured to connect to servers in Russia, and a programmer had hard-coded the Ukrainian national anthem into the database. The issues were corrected prior to deployment.¹⁴ (2023)

State and local election officials must prioritize enhanced defenses to protect voter registration databases and to limit the ways that compromised data can be exploited. Implementing and maintaining safeguards to prevent bad actors from using stolen data to successfully obtain absentee ballots, alter voter registration information, or add and delete registrants are essential for protection of the electoral process.

While the potential impact of voter registration database breaches is often minimized, these exploitations could have serious consequences for the administration of elections. The impact of the breaches is not limited to “undermining confidence” or “spreading false claims” but the data itself could be used months or years after the breach to alter voter registration information or request absentee ballots. **The real threat is what can be done with the stolen data.**

POTENTIAL AVENUES FOR EXPLOITATION

WHY IT MATTERS

OBTAINING ABSENTEE BALLOTS

In nearly every election jurisdiction, the information required to apply for and receive an absentee ballot is stored in the voter registration database. A breach can allow bad actors to access public information such as name, date of birth, and address but also sensitive information like driver's license numbers, full or partial social security numbers, and voter signatures on file. That information could enable bad actors to request absentee ballots at scale for low-propensity voters. Data obtained in a breach from 2021, for example, could be used to request a ballot for an election in 2028 because the data does not get stale.

ALTERING VOTER REGISTRATION INFORMATION OR DELETING REGISTRANTS

A malicious actor could use data from a breach to alter voter registration records to change addresses and therefore their polling place or change party affiliation to impede voting in an election. Perpetrated at scale, this type of exploitation could disenfranchise a significant number of voters, and if carefully distributed, such an attack might go unnoticed even if the scope was significant. This type of malicious alteration of voter data could be done over time using data obtained from a breach to log into official online state systems that enable voters to update their voter registration after passing identity checks using personal data like date of birth, portions of social security numbers, or driver's license number. Deletion of voter registration files could cause disruptions in the administration of elections if done at scale or, if executed in a distributed manner.

PREPAREDNESS IS THE BEST DEFENSE

DEVELOP A PLAN

Preparedness, built on a realistic threat assessment, is the foundation of effective election security measures. With a sober acknowledgment of the threat, state and local election officials can take steps to enhance the security of voter registration databases and absentee and mail ballots.

BACK UP DATABASE FILES REGULARLY

A commitment to good cybersecurity and best practices is critical to protecting voter registration data. States should schedule frequent, routine back-ups of the voter registration database files and store them securely offline. States should also test the ability to revert to back-up during an incident.

For jurisdictions that utilize electronic pollbooks, producing paper pollbooks as back-ups will limit the potential for disruptions on Election Day.

ENGAGE YOUR PLAN

If you detect unauthorized access to your voter registration database, immediately implement your security incident response plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your election resiliency and continuity plan.

PREPARE FOR POTENTIAL CYBERSECURITY INCIDENTS

Network infrastructure and internet-facing applications, including voter registration databases, underpin and enable a variety of functions in the conduct of elections. These may include election infrastructure networks that store, host, or process voter registration information, as well as public-facing election websites that support functions like polling place lookup. Local election officials have the power to prevent most security incidents using basic security measures. Take steps now so that even if an incident occurs, critical election operations can continue.

Protect and Respond: Phishing Attempts Targeting Your Email

- Enable Multifactor Authentication on all accounts.
 - Ensure each account has its own unique credentials and do not allow credential sharing.
 - Apply the principle of least privilege by separating admin accounts and user accounts.
 - Ensure everyone changes their default passwords and require strong passwords for all accounts.
- Enable Domain-based Message Authentication Reporting and Conformance for all email accounts to make it easier for email senders and receivers to determine whether an email legitimately originated from the identified sender and provides the user with instructions for handling the email if it is fraudulent.
- Implement flagging external emails to alert users to use due care when opening.
- Train staff so they know to only use their official email accounts, which often include enhanced security features, for official business.
- Train staff to spot and report phishing or other suspicious emails.
 - Malicious actors are improving their techniques all the time, so training should be provided at regular intervals to educate staff about the latest tactics and how to respond to suspicious communications. Regularly review common signs of phishing so staff are familiar with what to look out for and how to report.

Protect and Respond: Distributed Denial of Service Targeting Your Websites

- Review existing contracts and coordinate with both website service providers and internet service providers before an incident occurs.
 - Identify what additional Distributed Denial of Service (DDoS) mitigation and redundancy measures are available. Most major service providers have protections available, which may be offered at no cost for basic services, or at additional cost for advanced services.
 - Ensure you know who to contact in the event of an incident.
-

- Share information about important election dates and locations, requesting that ample troubleshooting is available during key periods, and ensuring mutual awareness of any planned maintenance that could impact election operations.
- Ensure network traffic monitoring and analysis is enabled via a firewall or intrusion detection system and that the logs are being reviewed.
- Have an alternate plan for information dissemination in case your website does go down. Make sure to test that plan.

Protect and Respond: Ransomware Targeting Your Network

- While not binding on non-Federal entities, CISA's Binding Operational Directives are indicative of best practices and network owners should consider following them.
- Develop a patch management plan that makes reducing the significant risk of known exploited vulnerabilities a top priority for remediation and requires critical vulnerabilities to be re-mediated within 15 calendar days of initial detection.
- Implement and enforce network segmentation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or moving laterally within an internal network. This includes not transferring election results on the business network.
- Implement endpoint detection and response software on endpoint devices to monitor for malicious traffic. Verify alerts are being created and response processes are followed.
- If not already being used, government entities should use .gov domains.
- Implement Malicious Domain Blocking and Reporting (MDBR) across your network devices to prevent IT systems from connecting to harmful web domains. MDBR can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.
- Develop and maintain incident response plans that specifically detail how to operate mission-critical processes in the event of a cybersecurity incident.
- Test your incident response plans with all key players who would be involved in implementing the response.
- Maintain backups that allow you to recover data at a minimum of up to 30 days prior.
 - Encrypt backup files and ensure credentials for accessing the backups are not stored in the targeted environment. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.
 - Ensure backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid.
 - Test the availability and integrity of backups in a disaster recovery scenario.

DATA BREACHES GENERALLY

Over the last decade, millions of Americans have had their personally identifiable information (PII) leaked in data breaches that are not related to voter registration but compromise election security, nonetheless. Cybercriminals have gained access to databases belonging to financial institutions, healthcare providers, and other government agencies, obtaining PII including Social Security numbers, addresses, full names, dates of birth, and driver's license numbers. In many cases, this information is sold on the dark web, where it is easily accessible to malicious actors. Because much of this same data is used to verify voter eligibility, maintain voter rolls, and verify identity for absentee ballot requests, large-scale PII exposure of data held by private companies has implications not only for privacy and financial fraud, but also for the integrity of U.S. elections.

- In July 2017, a credit reporting firm discovered a data breach that affected a potential 143 million United States citizens, almost half of the population. The breach reportedly began in May 2017 and was announced nearly four months later. By exploiting an unpatched vulnerability in web application software, cyber attackers were able to steal an unprecedented amount of PII including Social Security numbers, dates of birth, home addresses, driver's license numbers, and full names.
- On February 10, 2020, the Department of Justice (DOJ) indicted four members of China's People's Liberation Army on counts of economic espionage, wire fraud and computer fraud. In a statement following the indictment, Attorney General William Barr said the hack fits "a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."
- In April 2024, a background check firm that stored troves of records including full names, current and past addresses, Social Security numbers, dates of birth, and telephone numbers suffered a colossal data breach of 2.9 billion records containing PII of 170 million individuals. The information was reportedly found on the Dark Web being offered for \$3.5 million.
- One of the largest supplemental insurance providers in the United States suffered a data breach in June 2025 that affected 22.65 million individuals. Information accessed by hackers included PII such as Social Security numbers, dates of birth, driver's license numbers and full names. Hackers gained access to the provider's systems via social engineering tactics e.g. phishing, whaling, and impersonation.
- A report from the University of Oxford found that Russia and China ranked first and third, respectively, as nations that pose the highest threat level of cybercrime. Moreover, the PII available to these adversaries is not limited to that accessed through their own cyber operations but can be readily purchased or accessed on the dark web.

The cases mentioned above involve breaches that contained the information typically needed for voter registration and absentee ballot applications. The threat this exposed data poses to the integrity of U.S. elections is significant and ongoing, underscoring the need to recognize and mitigate the direct risk it poses to critical election infrastructure.

CONCLUSION

Voter registration databases are the foundation of our voting system. State and local election officials must prioritize system security and implement safeguards to prevent the exploitation of data that may have already been exposed. Adopting modern security enhancements such as smart network monitoring and multi-factor authentication can limit the risks of fraud and election disruptions. The Department of Homeland Security is charged with protecting the nation's critical infrastructure, including election infrastructure, and all state election officials are encouraged to collaborate with DHS on this important mission.

For more information about election security and resources to protect elections, visit the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Toolkit and Resources to Protect Elections page: [https:// www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections](https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections)

REFERENCES

¹ <https://www.justice.gov/archives/sco/file/1080281/dl?inline>

² <https://www.justice.gov/archives/sco/file/1080281/dl?inline>

³ [RIVERSIDE COUNTY: District attorney claims voters' party affiliations purposely changed without consent - Press Enterprise](https://www.justice.gov/archives/sco/file/1080281/dl?inline) ⁴
<https://www.justice.gov/archives/sco/file/1080281/dl?inline>

⁵ <https://www.justice.gov/archives/sco/file/1080281/dl?inline>

⁶ <https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-unitedstates-senate-russian-active-measures/>

⁷ [U.S. intel: Russia compromised seven states prior to 2016 election](https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-unitedstates-senate-russian-active-measures/)

⁸ [Voter Databases in Arizona and Illinois Breached, FBI Says](https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-unitedstates-senate-russian-active-measures/)

⁹ [GEORGIA VOTING HACK: FBI investigating alleged breach of Georgia elections center at Kennesaw State University - WSB-TV Channel 2 - Atlanta](https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-unitedstates-senate-russian-active-measures/)

¹⁰ https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

¹¹ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a>

¹² [Key Findings and Recommendations: Foreign Interference Related to the 2022 US Federal Elections | Homeland Security](https://www.dhs.gov/sites/default/files/2023-12/1_b_%20Memo%20DOJ%20and%20DHS%20Approved_508c.pdf)

¹³ https://www.dhs.gov/sites/default/files/2023-12/1_b_%20Memo%20DOJ%20and%20DHS%20Approved_508c.pdf

¹⁴ [Hacking Blind Spot: States Struggle to Vet Coders of Election Software - HSToday](https://www.dhs.gov/sites/default/files/2023-12/1_b_%20Memo%20DOJ%20and%20DHS%20Approved_508c.pdf)