Public Service Announcement

FBI & CISA

Alert Number: I-081424-PSA

August 15, 2024

Just So You Know: Ransomware Disruptions During Voting Periods Will Not Impact the Security and Resilience of Vote Casting or Counting

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to inform the public that while ransomware attacks against state or local government networks or election infrastructure could cause localized delays, they will not compromise the security or accuracy of vote casting or counting processes.

The threat of ransomware presents a critical challenge in today's digital landscape with malicious actors targeting individuals, businesses, and even infrastructure like government networks. Ransomware affecting state or local government systems could render certain election related functions temporarily inaccessible and cause election officials to revert to back-up processes and systems. While this could impact the speed of certain processes, it would not impact the security or accuracy of the processes around the casting and counting of votes. Election officials use a multi-layer approach to security that employs a variety of technological, physical, and procedural controls to prevent cyber intrusions, like ransomware, from impacting the security and resilience of vote casting and counting systems. In the event of a ransomware event affecting their offices, election officials have plans and redundancies in place to allow voting operations to continue so that all eligible voters are able to cast their ballot securely.

Any successful ransomware attack on election infrastructure tracked by the FBI and CISA has remained localized and successfully managed with minimal disruption to election operations and no impact on the security and accuracy of ballot casting or tabulation processes or systems.

In prior U.S. and foreign elections, malicious actors have sought to spread or amplify false or exaggerated claims about cyber incidents in an attempt to manipulate public opinion, discredit the electoral process, or undermine confidence in U.S. democratic institutions. As of the date of this report, the FBI and CISA have **no** reporting to suggest cyber activity, to include ransomware, has ever prevented a registered voter from casting a ballot, compromised the integrity of any ballots cast, or affected the accuracy of vote tabulation or voter registration information.

Recommendations for how to understand and mitigate the potential impacts of a ransomware incident on election infrastructure:

- Seek out information ahead of key deadlines or election day about registering to vote, polling locations, voting by mail, provisional ballot process, and final election results.
- Rely on state and local government election officials, as they are your trusted source of election information. Visit your state and local elections office websites for accurate information about the election process. Be cautious with websites not affiliated with local or state government. Some election officials have websites that use a ".gov" domain, indicating that they are an official government site. If you have questions about election security in your jurisdiction, contact your local election office directly.
- Remain alert to election-related schemes which may attempt to impede election administration or purport that there has been a cyber incident against election infrastructure or systems.
- Be cautious of social media posts and unsolicited emails or phone calls from unfamiliar email addresses or phone numbers that make suspicious claims about the elections process or cyber incidents against election infrastructure. If you receive or see this type of information, verify the information against the information provided by your state or local election official who are your trusted sources for election information.

The FBI and CISA coordinate closely with federal, state, local, and territorial election partners and provide services and information to safeguard U.S. voting processes and maintain the resilience of U.S. elections. The FBI is responsible for investigating and prosecuting election crimes, malign foreign influence operations, and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions. CISA, as the as the Sector Risk Management Agency for the Election Infrastructure subsector, helps critical infrastructure owners and operators, including those in the election community, ensure the security and resilience of election infrastructure from physical and cyber threats.

Victim Reporting and Additional Information

The FBI and CISA encourage the public to report information concerning suspicious or criminal activity, such as ransomware attacks, to their local FBI field office (www.fbi.gov/contact-us/field-offices-office), by calling 1-800-CALL-FBI (1-800-225-5324), or online at ic3.gov. Cyber incidents can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), mailing report@dhs.cisa.gov, or reporting online at cisa.gov/report.

For additional assistance, to include common terms and best practices, please visit:

- Stop Ransomware | CISA for additional resources to tackle ransomware more effectively.
- CISA #Protect2024 for additional resources to protect against the cyber, physical, and operational security risks to election infrastructure.
- Protected Voices for additional resources to protect against online foreign influence operations, cyber threats, and federal election crimes.