Public Service Announcement
FBI & CISA

October 04, 2022

Alert Number
I-100422b-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Malicious Cyber Activity Against Election Infrastructure Unlikely to Disrupt or Prevent Voting

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) assess that any attempts by cyber actors to compromise election infrastructure are unlikely to result in large-scale disruptions or prevent voting. As of the date of this report, the FBI and CISA have **no** reporting to suggest cyber activity has ever prevented a registered voter from casting a ballot, compromised the integrity of any ballots cast, or affected the accuracy of voter registration information. Any attempts tracked by FBI and CISA have remained localized and were blocked or successfully mitigated with minimal or no disruption to election processes.

The public should be aware that election officials use a variety of technological, physical, and procedural controls to mitigate the likelihood of malicious cyber activity (e.g., phishing, ransomware, denial of service, or domain spoofing) affecting the confidentiality, integrity, or availability of election infrastructure systems or data that would alter votes or otherwise disrupt or prevent voting. These include failsafe measures, such as provisional ballots and backup pollbooks, and safeguards that protect against voting malfunctions (e.g., logic and accuracy testing, chain of custody procedures, paper ballots, and post-election audits). Given the extensive safeguards in place and distributed nature of election infrastructure, the FBI and CISA continue to assess that attempts to manipulate votes at scale would be difficult to conduct undetected.

Election systems that house voter registration information or manage non-voting election processes continue to be a target of interest for malicious threat actors. Cyber actors may also seek to spread or amplify false or exaggerated claims of cybersecurity compromises to election infrastructure; however, these attempts would not prevent voting or the accurate reporting of results.[a]

The FBI and CISA will continue to quickly respond to any potential threats, provide recommendations to harden election infrastructure, notify stakeholders of threats and intrusion activity, and impose risks and

consequences on cyber actors seeking to threaten U.S. elections.

Recommendations

- For information about registering to vote, polling locations, voting by mail, provisional ballot process, and final election results, rely on state and local government election officials.
- Remain alert to election-related schemes which may attempt to impede election administration.
- Be wary of emails or phone calls from unfamiliar email addresses or phone numbers that make suspicious claims about the elections process or of social media posts that appear to spread inconsistent information about election-related incidents or results.
- Do not communicate with unsolicited email senders, open attachments from unknown individuals, or provide personal information via email without confirming the requester's identity. Be aware that many emails requesting your personal information often appear to be legitimate.
- Verify through multiple, reliable sources any reports about compromises of voter information or voting systems, and consider searching for other reliable sources before sharing such information via social media or other avenues.
- Be cautious with websites not affiliated with local or state government that solicit voting information, like voter registration information. Websites that end in ".gov" or websites you know are affiliated with your state or local election office are usually trustworthy. Be sure to know what your state and local elections office websites are in advance to avoid inadvertently providing your information to nefarious websites or actors.
- Report potential crimes—such as cyber targeting of voting systems—to your local FBI Field Office.
- Report cyber-related incidents on election infrastructure to your local election officials and CISA (Central@CISA.gov).

The FBI is responsible for investigating election crimes, malign foreign influence operations, and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions. CISA helps critical infrastructure owners and operators, including those in the election community, remain resilient against physical and cyber threats. The FBI and CISA provide services and information to uphold the security, integrity, and resiliency of U.S. election infrastructure.

Victim Reporting and Additional Information

The FBI and CISA encourages the public to report information concerning suspicious or criminal activity to their local FBI field office (www.fbi.gov/contact-us/field). For additional assistance, best practices, and common terms, please visit the following websites:

- FBI's Protected Voices: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices
- FBI's Election Crimes and Security: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security

- CISA's Election Security Resource Library: Election Security Library | CISA
- CISA's Stop Ransomware: https://www.cisa.gov/stopransomware
- CISA's Mis-, Dis-, and Malinformation Resource Library: https://www.cisa.gov/mdm-resource-library
- CISA's Election Security Rumor vs. Reality: https://www.cisa.gov/rumorcontrol

To access previously released 2020 election-related FBI/CISA PSAs, click on the IC3.gov links below:

- Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
- Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
- Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
- False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections

[a] Unless otherwise prohibited by law, U.S. persons linking, citing, quoting, or voicing the same arguments raised by malicious actors likely are engaging in First Amendment-protected activity. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect malign activity absent information specifically attributing the content to malicious actors. Malicious actors frequently amplify themes already present in lawful domestic debate. Lawful domestic actors in the United States have the right to use arguments originating from any source, even adversary narratives. This information should be considered in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties.