Public Service Announcement

FBI & CISA

23 September 2020

The FBI and CISA are issuing this PSA as a part of a series on threats to the 2020 election to enable the American public to be prepared, patient, and participating voters.

Cyber Threats to Voting Processes Could Slow But Not Prevent Voting

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to inform the public that attempts by cyber actors to compromise election infrastructure could slow but not prevent voting. The FBI and CISA have not identified any threats, to date, capable of preventing Americans from voting or changing vote tallies for the 2020 Elections. Any attempts tracked by FBI and CISA have remained localized and were blocked, minimal, or easily mitigated.

The FBI and CISA have **no** reporting to suggest cyber activity has prevented a registered voter from casting a ballot, compromised the integrity of any ballots cast, or affected the accuracy of voter registration information. However, even if actors did achieve such an impact, the public should be aware that election officials have multiple safeguards and plans in place—such as provisional ballots to ensure registered voters can cast ballots, paper backups, and backup pollbooks—to limit the impact and recover from a cyber incident with minimal disruption to voting. The FBI and CISA continue to assess that attempts to manipulate votes at scale would be difficult to conduct undetected.

Nevertheless, cyber actors continue attempts against election systems that register voters or house voter registration information, manage non-voting election processes, or provide unofficial election night reporting. These attempts could render these systems temporarily inaccessible to election officials, which could slow, but would not prevent, voting or the reporting of results.

The FBI and CISA will continue to quickly respond to 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 US elections.

Recommendations

- Seek out information from trustworthy sources.
- Always consider the source of voting information. Ask yourself, “Can I trust this information?”

- Seek out election information from trustworthy sources, verify who produced the content, and consider their intent. Remain alert to these and other schemes which may impact normal business practices.
- 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.
- 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.
- Report potential crimes—such as cyber targeting of voting systems—to the FBI.

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 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 the U.S. electoral processes.

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 to include: common terms and best practices, such as media literacy, please visit the following websites:

- Protected Voices: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices;
- Election Crimes and Security: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security; and
- #Protect2020: www.cisa.gov/protect2020.