Public Service Announcement
FBI & CISA

October 06, 2022

Alert Number
I-100622-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

Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are raising awareness of the potential threat posed by attempts to manipulate information or spread disinformation in the lead up to and after the 2022 midterm elections. Foreign actors may intensify efforts to influence outcomes of the 2022 midterm elections by circulating or amplifying reports of real or alleged malicious cyber activity on election infrastructure. Additionally, these foreign actors may create and knowingly disseminate false claims and narratives regarding voter suppression, voter or ballot fraud, and other false information intended to undermine confidence in the election processes and influence public opinion of the elections' legitimacy.[a,b] As with previous election cycles, foreign actors continue to knowingly spread false narratives about election infrastructure to promote social discord and distrust in U.S. democratic processes and institutions, and may include attempts to incite violence.

Foreign actors can use a number of methods to knowingly spread and amplify false claims and narratives about malicious cyber activity, voting processes, and results surrounding the midterm election cycle. These actors use publicly available and dark web media channels, online journals, messaging applications, spoofed websites, emails, text messages, and fake online personas on U.S. and foreign social media platforms to spread and amplify these false claims. For example, foreign actors may use such platforms to spread disinformation and claim successful cyber compromises of election infrastructure, evidenced by “hacked” or “leaked” U.S. voter registration data, suggesting compromise to the voting process or election result integrity. While some voter registration information is publicly available, the FBI and CISA have no information suggesting any cyber activity against U.S. election infrastructure has impacted the accuracy of voter registration information, prevented a registered voter from casting a ballot, or compromised the integrity of any ballots cast. These efforts by foreign actors aim to undermine voter confidence and to entice unwitting consumers of information and third-party individuals

to like, discuss, share, and amplify the spread of false or misleading narratives.

The FBI and CISA urge the American public to critically evaluate the sources of the information they consume and to seek out reliable and verified information from trusted sources, such as state and local election officials and reputable news media. The FBI and CISA will continue to quickly respond to potential threats, by seeking to engage with state and local officials and the public when possible.

Recommendations:

- For information about registering to vote, voting, and election results, rely on state and local government election officials.
- Visit the U.S. Election Assistance Commission website (https://www.eac.gov) as a resource for verified and reliable elections-related information and resources.
- Be aware that sensational content can be created or shared by foreign actors with the intent to incite anger, mobilize, and to promote amplification of false information.
- Seek information from trustworthy and reputable media and social media sources, considering the author and their intent.
- Keep in mind that some news sites sound authentic but are authored by foreign actors.
- Confirm with reputable sources, reports that claim voting or elections infrastructure challenges or discrepancies. Know where to access local election information, such as official websites, official social media accounts, or by contacting local elections officials.
- Critically evaluate the information you share, and verify information with trusted sources, such as state and local election officials and reputable news media. If the information is not from a credible source or if a second reliable source cannot be found, consider not sharing it as you may be inadvertently amplifying misinformation.
- Be wary of phone calls or emails from unfamiliar callers and senders that make suspicious claims about the elections process or of social media posts that appear to spread inconsistent information about election-related problems or results.
- If appropriate, make use of in-platform tools offered by social media companies for reporting elections related disinformation.
- 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 election crimes—such as intentional disinformation about the manner, time, or place of voting—to your local FBI Field Office.

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 the public and private sector to uphold the security, integrity, and resiliency of U.S. election infrastructure.

Victim Reporting and Additional Information

The FBI and CISA encourage 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 and see previous FBI Public Service Announcements (PSAs):

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

To access the recently released 2022 midterm election-related FBI/CISA PSA, click on the IC3.gov link below:

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

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

- 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
- 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

[a] Reference 18 U.S. Code **§** 594.

[b] 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. 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.