Elections Infrastructure ISAC®

OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN FOCUS

7 OCTOBER 2024 DHS-IA-IF-2024-01980

CYBERSECURITY

(U//FOUO) Cyber Criminals More Likely To Disrupt US Elections Infrastructure Than Nation-State-Affiliated Cyber Actors, Who Likely Favor Espionage

(U//FOUO) **Financially and ideologically motivated cyber criminals are more likely than nation-state-affiliated cyber actors to attempt to disrupt elections infrastructure, potentially creating localized delays and interruptions to election-related processes and networks.**[a] Since the 2022 midterm elections, financially and ideologically motivated cyber criminals have targeted US state and local government entity networks that manage or support election processes. In some cases, successful ransomware attacks and a distributed denial-of-service (DDoS) attack on such infrastructure delayed election-related operations in the affected state or locality but did not compromise the integrity of voting processes. We have no evidence that any foreign government-affiliated actor or cyber criminals prevented voting, altered any technical aspect of the voting process, or otherwise compromised the integrity of voter registration information for any ballots cast, according to a joint report from DHS and DOJ.

- *(U//FOUO)* Since at least 2022, financially motivated cyber criminal attacks have delayed election-related processes using ransomware attacks or by driving victims to remediate an attack, judging from DHS reporting. For example, in 2022, ransomware actors probably inadvertently prevented a US county from accessing its network and almost caused the county to miss the legal deadline to mail ballots to voters, according to open-source reporting. Similarly, in March 2024, a different US county experienced a ransomware attack that forced it to purchase

[a] *(U)* **Elections infrastructure** includes but is not limited to: voter registration databases and associated information technology (IT) systems; IT infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results and post-election reporting to certify and validate results); voting systems and associated infrastructure; storage facilities for election and voting system infrastructure; polling places, to include early voting locations; and other systems to manage election processes.

new network devices and re-connect to the state-level election system, according to DHS reporting.

- *(U//FOUO)* Ideologically motivated cyber criminals—or criminal hacktivists—and other unidentified cyber criminal actors have probably intentionally disrupted or gained unauthorized access to US election-related networks, judging from a review of DHS reporting from January 2022 through May 2024. For example, a pro-Russia criminal hacktivist group claimed responsibility for a confirmed DDoS attack that resulted in temporarily restricted access on a public-facing US state's secretary of state website on Election Day 2022, according to DHS and open-source reporting. In early 2024, a separate pro-Russian criminal hacktivist group briefly posted its intention to target the 2024 US election, according to open-source reporting, although we have no reporting to suggest the actor ultimately carried out an attack.

- *(U)* Nation-state-affiliated cyber actors have not attempted to disrupt US elections infrastructure, despite reconnaissance and occasionally acquiring access to non-voting infrastructure. In 2016, Russia almost certainly reconnoitered election networks in all US states and accessed election-related infrastructure in at least two states, according to a declassified US Intelligence Community (IC) report. During the 2020 US election cycle, Iranian, People's Republic of China (PRC), and Russian government-affiliated actors materially impacted the security of networks associated with or pertaining to US political organizations, candidates, and campaigns, according to a joint report from DHS and DOJ.

(U//FOUO) **In contrast to financially and ideologically motivated cyber criminals, nation-state-affiliated cyber actors likely view US state and local government and political campaign networks as potential targets for cyber-enabled espionage and malign influence operations.** US state and local government networks often contain data repositories, such as voter registration databases or election management systems, which contain personally identifiable information (PII) for registered voters. US political campaign networks contain internal communications and may also contain voter information obtained legitimately from election offices or from publicly available sources. Foreign adversaries, such as Iran, the PRC, and Russia, have conducted cyber operations against the networks of US state and local governments and US political campaigns; a successful compromise of these networks may provide nation-state-affiliated cyber actors with options for subsequent cyber-enabled malign influence operations, as previously observed in 2016 and 2020.

- *(U//FOUO)* Russian and Iranian state-affiliated cyber actors have compromised the networks of US state and local governments and political campaigns, exfiltrated sensitive information and data, and used such information to enrich their capabilities to conduct cyber-enabled malign influence operations. During the

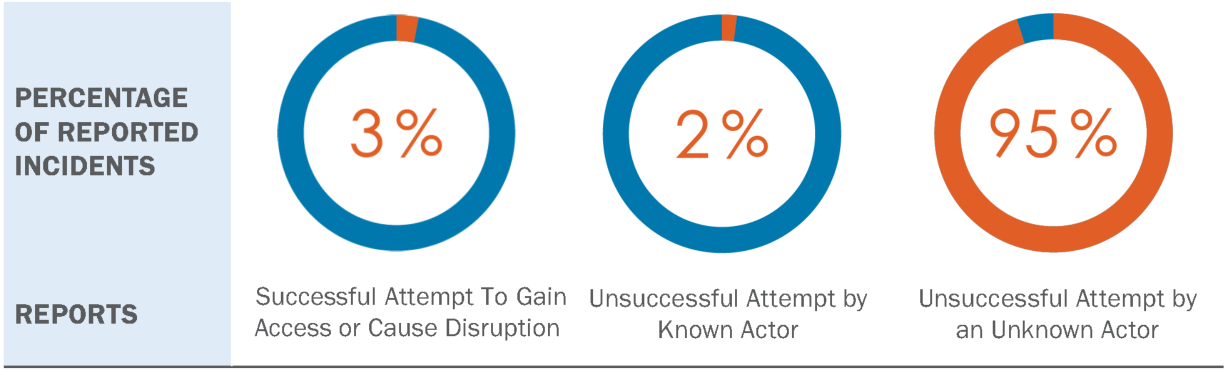
2024 US elections, Iranian state-affiliated cyber actors reportedly compromised a US presidential campaign and unsuccessfully attempted to leak internal campaign documents through US news outlets, judging from US government and open-source reporting. During the 2020 US elections, Iranian state-affiliated cyber actors compromised at least one US elections infrastructure entity, stole US voter information, and sent threatening e-mails to intimidate US voters, according to an FBI report. During the 2016 US election cycle, Russian state-affiliated cyber actors compromised the election-related networks of US state and local governments and political campaign networks, stole information, and publicly released stolen information in an effort to influence the election, according to a declassified IC report.

- *(U//FOUO)* In 2022, PRC cyber actors probably sought to collect PII and other data on US voters, according to US government reporting. For example, in the lead-up to the 2022 US elections, PRC cyber actors collected publicly available US voter information, according to US government reporting. The PRC has also conducted reconnaissance on the websites of US state and local governments and political parties during the 2022 US election cycle. PRC cyber actors could leverage this information in future cyber or influence operations, although we lack indications of planned operations.

OVERALL GRAPHIC CLASSIFICATION: UNCLASSIFIED

(U) 2022–2024 DHS Cyber Threats to Elections Reporting

(U) Unknown actors conducted the vast majority of reported malicious cyber activity. DHS, FBI, and EI-ISAC recommend elections community entities promptly report cyber incidents and malicious cyber activity.



DHS-IA-IF-2024-01980

24-384-IA

(U//FOUO) **Regular engagement with federal partners on cyber threats, common cybersecurity practices, and mitigations likely would reduce the impact and scale of cyber attacks on US elections infrastructure.** Continued adoption and maturation of essential cyber hygiene practices can reduce the impact of potential direct or indirect threats, and rapidly sharing information can help identify potential vulnerabilities and the scope of future cyber campaigns. This information can be provided to network defenders across the country to identify, triage, and mitigate potential threats.

- *(U)* Increased information sharing between US state and local election officials and federal partners can help mitigate potentially higher impact incidents such as ransomware attacks. Ransomware victims who solicited federal assistance to address ransomware attacks significantly decreased the duration and impact of the attack, according to a reputable IT firm’s 2023 reporting. CISA and FBI recommend promptly reporting ransomware attacks via their respective portals and hotlines.[b] State and local election officials can also report ransomware incidents to the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), a nonprofit organization partially funded by CISA to improve the cybersecurity posture of US election offices.
- *(U//FOUO)* Routine reports of cyber actors conducting activity on US state and local election boards, election officials’ e-mail accounts, and county networks used by election officials to support the management of elections have filled vital community information sharing needs, such as cyber threat indicators, cyber actor tactics, and the impacts of cyber incidents, according to DHS reporting. Examples of successful compromise include unknown criminal actors leveraging vulnerabilities in a web application to gain unauthorized access to a secured website for a US state board of elections and exploiting unsecured cloud storage to steal sensitive poll workers’ data, according to DHS reporting.
- *(U//FOUO)* US state and local governments can benefit from CISA resources to improve their cybersecurity postures. In FY 2023, CISA observed that newly enrolled elections infrastructure entities decreased their exposed vulnerabilities by an average of 10 percent within the first three months of using CISA’s vulnerability scanning service.

[b] *(U)* See resources available in Appendix A.

(U//FOUO) Decentralized Nature of National Elections Infrastructure Reduces Scale of Cyber Attack Impacts

(U//FOUO) Malicious cyber operations disrupting the underlying infrastructure that supports election processes can directly or indirectly impact elections infrastructure or processes. The interconnected nature of US state and local government networks, some of which are used to manage government services and data that include elections functions, expands the attack surface for cyber actors. However, the decentralized nature of national elections infrastructure and operations—such as the administration of voting systems, state and local election policies, and varying degrees of internet-facing infrastructure used to support elections nationwide—can help mitigate the impact of any cyber-enabled disruption.

(U) Appendix A: Reporting Cyber Incidents to CISA and FBI

(U) Potential cyber incidents can have serious consequences for critical infrastructure and election operators. Elections infrastructure stakeholders encountering a cyber incident should promptly report the activity to CISA and FBI. The FBI and CISA respond to reported incidents by providing threat response and resource coordination. The federal government can provide resources to support state and local entities in identifying, triaging, and recovering from potential incidents, including sharing actionable information with other critical infrastructure network defenders to make proactive risk-informed decisions to safeguard their infrastructure.

(U) Elections infrastructure stakeholders can quickly request assistance from CISA by contacting CISA Central to get up-to-date information and understand the evolving risk landscape:

- *(U)* Call 1-844-Say-CISA or 844-729-2472
- *(U)* E-mail report@cisa.gov
- *(U)* Report online at https://www.cisa.gov/report

(U) The FBI encourages elections infrastructure stakeholders to report suspicious activity to their local FBI field office:

- *(U)* Visit https://www.fbi.gov/contact-us/field-offices
- *(U)* Call 1-800-CALL-FBI (1-800-225-5324)
- *(U)* Report online at https://www.tips.fbi.gov/home

(U) Appendix B: CISA's Essential Risk Mitigation Strategies for Elections Infrastructure Owners and Operators

(U) Elections infrastructure owners and operators can further improve election-related infrastructure security and resilience by pursuing opportunities for action outlined below. CISA encourages elections infrastructure entities to leverage CISA's no-cost, voluntary resources to identify and mitigate potential vulnerabilities. The recommended practices below align with CISA's Cybersecurity Performance Goals (CPGs).

- *(U)* Ensure election organizations have, maintain, update, and practice incident response plans to quickly identify, contain, mitigate, and communicate cybersecurity incidents. (CISA CPG 2.S)
- *(U)* Enroll in cyber hygiene services through regional CISA Election Security Advisors.
- *(U)* Routinely patch systems and assets and remediate all Known and Exploited Vulnerabilities immediately, prioritizing critical assets first. Entities should refer to vendor mitigation guidance and implement compensating controls if a system or assets cannot be patched. (CISA CPG 1.E)
- *(U)* Implement network segmentation to isolate critical systems from the broader organization network to reduce the likelihood of a compromise, and only allow connections from approved assets. (CISA CPG 2.F)
- *(U)* Strengthen account security by implementing phishing-resistant multi-factor authentication; separating user and privileged accounts; and adopting strong, complex passwords throughout the organization. (CISA CPGs 2.A, 2.B, 2.C, 2.D, 2.E, 2.G, 2.H, and 2.I)
- *(U)* Ensure critical election systems and resources are backed up on a regular basis. System backups should be stored separately from the source systems, encrypted, and tested on a recurring basis. (CISA CPG 2.R)

(U) For more information on how to align with these baseline practices, please visit https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

(U) **Cybersecurity Resources**

(U) For additional no-cost resources, please refer to the following:

(U) CISA's #Protect2024 site is a centralized location for resources to protect elections infrastructure: https://www.cisa.gov/topics/election-security/protect2024

(U) CISA's StopRansomware site is a centralized location for information and resources: https://www.cisa.gov/stopransomware

(U) The FBI's Protected Voices site provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations, cyber threats, and federal election crimes: https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

(U) The EI-ISAC's Election Security Tools and Resources site provides resources to support the cybersecurity needs of the election community: https://www.cisecurity.org/elections

Source, Reference, and Dissemination Information

Definitions	(U) **Criminal Hacktivist:** An individual or group who gains unauthorized access to computer files or networks in order to further social or political goals, wholly or in part, through unlawful acts or criminal cyber activity. (U) **Financially Motivated Cyber Actors:** Cyber criminal actors who are predominantly driven by financial gain and tend to choose targets opportunistically. (U) **US State Secretary of State:** US state government official who is often the chief election official in a US state.
Reporting Suspicious Activity	(U) **To report a computer security incident, either contact CISA at 888-282-0870, or go to https://www.cisa.gov/forms/report/ and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Warning Notices & Handling Caveats	(U) **Warning:** This information is provided only for intelligence purposes in an effort to develop potential investigative leads. It cannot be used in connection with any foreign or domestic court proceedings or for any other legal, judicial, or administrative purposes. (U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. (U) All US person information has been minimized. Should you require US person information, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Cyber Criminals More Likely To Disrupt US Elections Infrastructure Than Nation-State-Affiliated

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- □ Drive planning and preparedness efforts, training, and/or emergency response operations
- □ Observe, identify, and/or disrupt threats
- □ Share with partners
- □ Allocate resources (e.g. equipment and personnel)
- □ Reprioritize organizational focus
- □ Author or adjust policies and guidelines
- □ Initiate a law enforcement investigation
- □ Intiate your own regional-specific analysis
- □ Intiate your own topic-specific analysis
- □ Develop long-term homeland security strategies
- □ Do not plan to use
- □ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:

Position:

Organization:

State:

Contact Number:

Email:

Submit Feedback

Privacy Act Statement