OFFICE of INTELLIGENCE and ANALYSIS

REFERENCE AID

19 OCTOBER 2020 IA-45700-21

CYBERSECURITY

(U//FOUO) Cyber Threats to Critical Dependencies of Election Infrastructure

(U//FOUO) This *Reference Aid* provides DHS, federal, state, local, and private sector stakeholders an overview of cyber threats to election infrastructure through the lens of the critical dependencies that support the functions of conducting elections. This product also includes examples of cyber actors conducting reconnaissance, accessing networks, exfiltrating data, or disrupting a component of that critical dependency. We selected the critical dependencies based on consultation with the DHS Cybersecurity and Infrastructure Security Agency and an analysis of the systems, networks, services, and technologies that underpin the national critical functions that enable election operations.[a] This product is not intended to address supply chain dependencies of election infrastructure, such as the manufacture of voting or tabulation machines and their components. Although voting facilities include both commercial and government facilities sectors, they depend on electricity and internet service, which are captured in this product.

(U) Overview of US Election Infrastructure

(U) Election infrastructure comprises a diverse set of systems, networks, and processes, including voter registration, pollbooks, voting machines, tabulation, and election websites. Each jurisdiction's election infrastructure ecosystem is a collection of different components, some interconnected electronically and others not, that must function together to conduct elections.

[a] (U//FOUO) For additional insight on threats to election infrastructure see *(U//FOUO) Cyber Threats to US Election Infrastructure (IA-33173-19), dated 14 June 2019,* and *(U) Cybercriminals and Criminal Hackers Capable of Disrupting Election Infrastructure (IA-44389-19), dated 29 July 2020.*

Homeland Security

OFFICE OF INTELLIGENCE & ANALYSIS

OCTOBER 2020

(U//FOUO) Cyber Threats to Critical Dependencies of Election Infrastructure

(U//FOUO) This product provides an overview of critical dependencies of US election infrastructure and incidents where malicious cyber actors compromised, disrupted, or destroyed components of the dependencies in the United States or overseas as exemplars of some of the activity that could occur prior to an election. We have observed foreign adversaries and criminal actors target US critical infrastructure, particularly nation-state cyber actors engaged in broad efforts against the information technology and energy sectors, as well as cyber actors targeting sectors such as transportation and communications with financially driven ransomware and other malware. The most prevalent threat to critical infrastructure networks that support the functions of conducting elections and election infrastructure likely is ransomware, based on an observed 153 percent increase in the number of reported state and local government ransomware attacks from 2018 to 2019.

(U) CRITICAL INFRASTRUCTURE SECTOR	(U) CRITICAL DEPENDENCIES	(U) ELECTION-RELATED OPERATION	(U) EXAMPLE	(U) CISA-RECOMMENDED MITIGATION
(U) Information Technology Sector/ Network Infrastructure Devices	(U) Managed Service Provider	(U//FOUO) Managed service providers (MSPs) remotely host the information technology infrastructure of state and local government networks that support file systems and services related to aspects of election infrastructure.	• (U) August 2019: A ransomware attack on a Texas-based MSP used by local government agencies across 22 municipalities caused city courts, police departments, and county offices to lose access to e-mail, billing, and scheduling systems. • (U) December 2018: The Department of Justice indicted two cyber actors associated with the Chinese Ministry of State Security for their involvement in a global campaign targeting the networks of MSPs. By leveraging MSP networks, the actors gained unauthorized access to the computers and networks of MSP clients to steal IP addresses, confidential business information, and other data from more than 45 companies in at least a dozen US states and US government agencies.	• (U) Understand the supply chain risk associated with MSPs, particularly in cases where MSP clients do not conduct a majority of their own network defense. • (U) For an overview of tactics, techniques, and procedures used by advanced persistent threat actors in MSP network environments and mitigation techniques see *(U) Advanced Persistent Threat Activity Exploiting Managed Service Providers (TA 18-276B), dated 3 October 2018.*
(U) Communications Sector	(U) Internet Service Provider	(U) Internet service providers (ISPs) provide internet connections and services to election-related organizations and public and private sector entities, including state and local internet-connected election systems--such as voter lookup tools or election night reporting mechanisms.	• (U//FOUO) July 2020: Unidentified cyber actor(s) conducted a successful distributed denial-of-service (DDoS) attack against a US city government's information technology infrastructure, disrupting essential services for several hours. The attack targeted domain name system servers to disable all public-facing services, virtual private network connections, and mobile devices, including telework and police services.	• (U) Enroll in denial-of-service protection services that detect abnormal traffic flows and redirect traffic away from their networks. • (U) Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack. Contact the ISP to advise on an appropriate course of action. • (U) For recommended mitigation techniques see *(U) Security Tip: Understanding Denial-of-Service Attacks (ST04-015), dated 20 November 2019.*
(U) Transportation Systems Sector	(U) US Postal Service/Mail Processing and Handling Equipment	(U) The US Postal Service (USPS) and mail processing facilities support outbound and inbound processes of mail ballots, including a barcoding system that enables ballot tracking. Operational technology connected to US address and zip code directory databases support barcoding and sort programs.	• (U) May 2020: A US mail automation and technology firm was targeted by MAZE ransomware. The company reported it was able to thwart the attack before data could be encrypted. There was no evidence of further unauthorized access to the firm's IT system. • (U) October 2019: A US mail automation and technology firm was infected by Ryuk ransomware that encrypted information and disrupted sortation facility operations and clients' access to services for several days. • (U) November 2014: Sophisticated cyber actors exfiltrated sensitive personal information of more than 800,000 employees, as well as data on customers who called or e-mailed the USPS. USPS restricted network communications with the internet for one to two days until security upgrades could be made.	• (U) Focus on cyber risk management activities, including access controls and authentication best practices when implementing expanded mail-in voting. • (U) For specific compensating controls for the mail-in voting process see *(U) Mail-In Voting in 2020 Infrastructure Risk Assessment, dated 28 July 2020.*
Energy Sector	(U) Power Grid	(U) The energy sector supports electronic voting infrastructure, including the use of electronic pollbooks, direct record electronic (DRE) voting machines, tabulation processes, and the submission of results.	• (U) December 2016: Russian actors used custom malware designed to gain control of electrical substations, enabling the actors to disrupt the power supply to parts of Kyiv, Ukraine, for several hours. • (U//FOUO) March 2016: Russian Government cyber actors targeted US energy sector networks through a multi-stage intrusion campaign to conduct network reconnaissance, move laterally, and collect information pertaining to industrial control systems (ICSs). The actors on at least one occasion gained accessed to the human machine interface (HMI) via the corporate network. The HMI provides ICS operators with a graphical interface to monitor and control the ICS. There was no indication that the actors attempted to control the HMI; however, they had access to do so. • (U) December 2015: Russian actors targeted two Ukrainian energy distribution companies with malware (BlackEnergy 3), allowing the actors to interact remotely with control systems to disrupt the supply of electricity to more than 230,000 Ukrainian residents. The actors also conducted a telephonic denial-of-service attack on the energy company's call center to deny access to customers reporting outages.	• (U) Consider system outages in contingency plans and develop mitigation measures to ensure election processes can continue even in the event of electricity outages. Mitigation recommendations include use of paper ballots and provisional ballots.

Source, Reference, and Dissemination Information	
Reporting Suspicious Activity	*(U)* To report a computer security incident please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs 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. *(U)* To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Dissemination	*(U)* Federal, state, local, tribal, and territorial authorities and private sector stakeholders.
Warning Notices & Handling Caveats	*(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.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Cyber Threats to Critical Dependencies of Election Infrastructure

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 Disgree	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

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**