INTELLIGENCE ASSESSMENT

(U//FOUO) Cyber Threats and Vulnerabilities to US Election Infrastructure

20 September 2016

Homeland Security

National Protection and Programs Directorate

Office of Intelligence and Analysis

IA-0213-16

Homeland Security
Office of Intelligence & Analysis
National Protection and Programs Directorate
INTELLIGENCE ASSESSMENT
20 September 2016

(U//FOUO) Cyber Threats and Vulnerabilities to US Election Infrastructure

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A) and the Office of Cyber and Infrastructure Analysis (OCIA).

(U) Scope

(U//FOUO) This *Assessment* provides a baseline understanding of cyber threats to computer-enabled US election infrastructure. This *Assessment* discusses cyber risk and provides mitigation measures to owners and operators of US election infrastructure. This *Assessment* is intended to assist state and local governments in protecting, preventing, mitigating, and responding to cyber incidents against US election infrastructure.

(U) Key Judgments

(U//FOUO) DHS has no indication that adversaries or criminals are planning cyber operations against US election infrastructure that would change the outcome of the coming US election. Multiple checks and redundancies in US election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results—make it likely that cyber manipulation of US election systems intended to change the outcome of a national election would be detected.

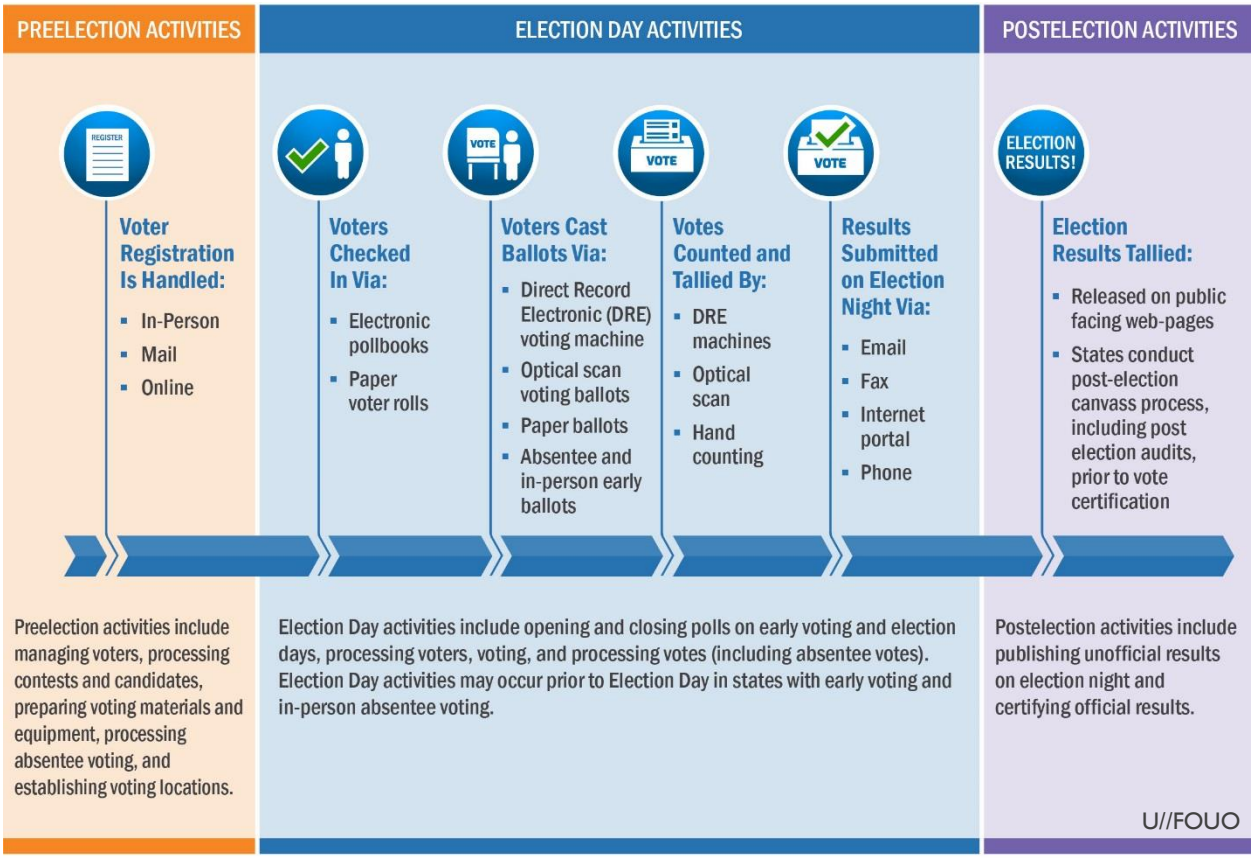
(U//FOUO) We judge cybercriminals and criminal hackers are likely to continue to target personally identifiable information (PII), such as that available in voter registration databases. We have no indication, however, that criminals are planning theft of voter information to disrupt or alter US computer-enabled election infrastructure.

(U//FOUO) We assess multiple elements of US election infrastructure are potentially vulnerable to cyber intrusions. The risk to US computer-enabled election systems varies from county to county, between types of devices used, and among processes used by polling stations.

(U) US Computer-Enabled Election Infrastructure

(U) US election infrastructure is a diverse set of assets, systems, and networks, both public and private. Based on our analysis of each phase of the election process, the following election infrastructure represents the key computer-enabled assets, systems, and networks most critical to the security and resilience of the election process.

- *(U) Electronic voting systems and associated infrastructure located at polling places during voting.*
- *(U) Information technology infrastructure and systems used to maintain voter registration databases.*
- *(U) Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night, as well as for post-election reporting used to certify and validate results.*



(U) Election Processes: Some Computer-Enabled

(U//FOUO) No Indication of Cyber Operations to Change Vote Outcome

(U//FOUO) DHS has no indication that adversaries or criminals are planning cyber operations against US election infrastructure that would change the outcome of the coming US election. Multiple checks and redundancies in US election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaigns and election officials to check, audit, and validate results—make it likely that cyber manipulation of US election systems intended to change the outcome of a national election would be detected.

» (U//FOUO) We assess that successfully mounting widespread cyber operations against US voting machines, enough to affect a national election, would require a multiyear effort with significant human and information technology resources available only to a nation-state. The level of effort and scale required to change the outcome of a national election, however, would make it nearly impossible to avoid detection. This assessment is based on the diversity of systems, the need for physical access to compromise voting machines, and the security and pre-election testing employed by state and local officials.* In addition, the vast majority of localities engage in logic and accuracy testing, which work to ensure voting machines operate and tabulate as expected—before, during, and after the election.

» (U//FOUO) We judge, as a whole, voter registration databases are resilient to systemic, nationwide cyber manipulation because of the diverse systems and security measures surrounding them. Targeted intrusions against individual voter registration databases, however, are possible. Additionally, with illicit access, manipulation of voter

* (U) Voting precincts in more than 3,100 counties across the United States use nearly 50 different types of voting machines produced by 14 different manufacturers. The diversity in voting systems and versions of voting software provides significant security by complicating attack planning. Most voting machines do not have active connections to the Internet.

data, or disruptions to their availability, may impact a voter's ability to vote on Election Day. Most jurisdictions, however, still rely on paper voter rolls or electronic poll books that are not connected in real-time to voter registration databases, limiting the possible impacts in 2016.

» (U//FOUO) We assess the impact of an intrusion into vote tabulation systems would likely be contained to the manipulation of unofficial Election Night reporting results, which would not impact the certified outcome of an election, but could undermine public confidence in the results. In addition, local election officials, media organizations, and political campaigns carefully monitor local voting patterns, particularly in electorally significant jurisdictions, and are likely to detect and begin investigating potential anomalies quickly.

(U//FOUO) Non-State Actors Likely To Continue Targeting PII, Potentially Attempt Disruption

(U//FOUO) We judge cybercriminals and criminal hackers are likely to continue to target voter PII. We have no indication, however, that cybercriminals are planning theft of voter information to disrupt or alter computer-enabled US election infrastructure voting. Politically-motivated criminal hackers could attempt temporary disruptive cyber attacks, such as denial-of-service (DoS) attacks or web defacements against election-related websites, in the lead-up to or during the election process. Disruptive attacks could target public-facing state and local government websites, potentially including election infrastructure used to report election results to the general public and media; however, we judge this activity would likely have little impact on the voting process itself.

» (U//FOUO) Unknown cyber actors in mid-July used an open-source scanning tool to identify and exploit a structured query language (SQL) injection vulnerability and exfiltrate PII from a Midwestern state board of elections website, according to FBI sources with excellent access and information provided by a cybersecurity organization supporting states. In at least three other states, voting and non-voting related websites during the same period observed unsuccessful SQL injection attacks from unknown actors, according to the same reporting.

» (U//FOUO) Cybercriminals routinely attempt exploitation of misconfigured and vulnerable websites and webservers via SQL injection, brute force login attempts, cross-site scripting, and other publicly known vulnerabilities, according to DHS reporting from sources with direct access.

» (U//FOUO) Criminal hackers routinely engage in disruptive attacks such as website defacement and DoS attacks, through exploiting publicly known vulnerabilities and for-hire DoS tools, according to DHS reporting from reliable sources with direct access.

(U) Vulnerability of Computer-Enabled Election Systems

(U//FOUO) We assess multiple elements of US election infrastructure are potentially vulnerable to cyber intrusions. The risk to computer-enabled election systems, however, varies from county to county, between types of devices used and among processes used by polling stations.

» (U//FOUO) **Electronic Voting Systems**: Security researchers have repeatedly demonstrated in laboratory testing environments that voting machines are vulnerable to compromise, usually with physical access, and such compromises could result in the manipulation of vote totals. Election outcomes would only be impacted if the compromise happened on a large scale across multiple machines or jurisdictions—which we judge to be beyond the capability of any adversary—or in cases of smaller local elections where the margin of victory is at a smaller scale.

» (U//FOUO) **Voter Registration Databases**: Online voter registration systems provide a potential point of vulnerability to enable cyber actors to gain illicit access to voter registration databases. Cyber actors have exploited these portals in the past to gain illicit access to voter information. Compromises of voter registration databases have resulted in the potential release of PII, but not the modification of records—with the exception of one unconfirmed incident of voter registration manipulation reported by US media. The exposure of voters' information would have limited impact on the integrity of the election process; however, it could undermine confidence in the system and provide the ability to conduct further cyber operations.

» (U//FOUO) **Public Dissemination of Voting Results**: State government information technology solutions generally include a public-facing Internet-connected portion that is used to report election results to the general public and media, which some states have begun migrating to the cloud due to Election Day demand. Vulnerabilities in the public-facing Internet portion could be used to display inaccurate vote results to the public and media. Election Day results are not the official results of the state or local jurisdiction.

(U) For further references please see Attachments:

1) (U) US-CERT – Securing Voter Registration Data [Security Tip (ST16-001)], published 15 September 2016, available at https://www.us-cert.gov/ncas/tips/ST16-001
2) (U) USG – Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government, available at https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf
3) (U) NPPD – State, Local, Tribal, and Territorial (SLTT) Cybersecurity Engagement

(U) Source Summary Statement

(U//FOUO) This Assessment *is based on DHS, FBI, and US media reporting, as well as our understanding of cyber actors and their capabilities. We assess these sources provide credible information based on their direct access to the reported information. We have* ***moderate confidence*** *in our assessment that adversaries or criminals are not planning cyber operations that would compromise the vote integrity of the coming election, attempt theft, or conduct short-lived disruptive cyber incidents.*

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. 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) Tracked by: HSEC-1.1, HSEC-1.2, HSEC-1.3