CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

July 28, 2020; 1400 EDT.

ELECTION INFRASTRUCTURE CYBER RISK ASSESSMENT

Fair and free elections are a hallmark of American democracy. The American people's confidence in the value of their vote is reliant on their confidence in the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and one of the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA's) highest priorities. CISA is working collaboratively in coordination with our federal partners, with those on the front lines of elections—state and local governments, election officials, and vendors—to manage risks to the Nation's election infrastructure. In this paper, CISA assesses risk to election infrastructure in order to assist the election community in understanding and managing risk to their critical systems.

To complete this work, CISA's National Risk Management Center (NRMC) assessed multiple criteria that quantify the scale of election infrastructure cyber risk, including machine preparation, device networking, and the centralization of infrastructure components. CISA NRMC also assessed additional risk criteria related to voter registration, voting machines, and electronic submission of ballots.

KEY FINDINGS

Compromises to the integrity of state-level voter registration systems, the preparation of election data (e.g., ballot programming), vote aggregation systems, and election websites present particular risk to the ability of jurisdictions to conduct elections.

When proper mitigations and incident response plans are not in place, cyber attacks on the availability of state or local-level systems that support same day registration, vote center check-in, or provisional voting also have the potential to pose meaningful risk on the ability of jurisdictions to conduct elections.

While compromises to voting machine systems present a high consequence target for threat actors, the low likelihood of successful attacks at scale on voting machine systems during use means that there is lower risk of such incidents when compared to other infrastructure components of the election process.

U.S. election systems are comprised of diverse infrastructure and security controls, and many systems invest significantly in security. However, even jurisdictions that implement cybersecurity best practices are potentially vulnerable to cyber attack by sophisticated cyber actors, such as nation-state actors.

Disinformation campaigns conducted in concert with cyber attacks on election infrastructure can amplify disruptions of electoral processes and public distrust of election results.

SCOPE NOTE: The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center (NRMC) prepared this risk assessment to support CISA efforts to help U.S. state and local governments mitigate vulnerabilities to election systems, and support cybersecurity and system resilience within election systems. This product provides base-level analysis election officials can use to prioritize and tailor risk management efforts to address specific vulnerabilities in high consequence election system components, and to promote cybersecurity and system resilience within election systems. Prioritizing mitigation of risk to potential cyber attacks on the integrity of election system components could yield the greatest marginal benefit in improving states' risk profiles.

CISA NRMC coordinated this analysis with the CISA Cybersecurity Division (CSD) and DHS's Office of Intelligence and Analysis (I&A) Cyber Mission Center (CYMC).

ELECTION INFRASTRUCTURE SYSTEMS OVERVIEW

Election infrastructure is comprised of a diverse set of systems, networks, and processes. The election system in the United States is not one system, but a collection of many different systems. 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. Although they perform the same functions, system processes and infrastructure vary from state-to-state and often differ even between counties, parishes, towns, or cities within a state or territory.[1]

Figure 1 provides a functional overview of a U.S. election ecosystem.

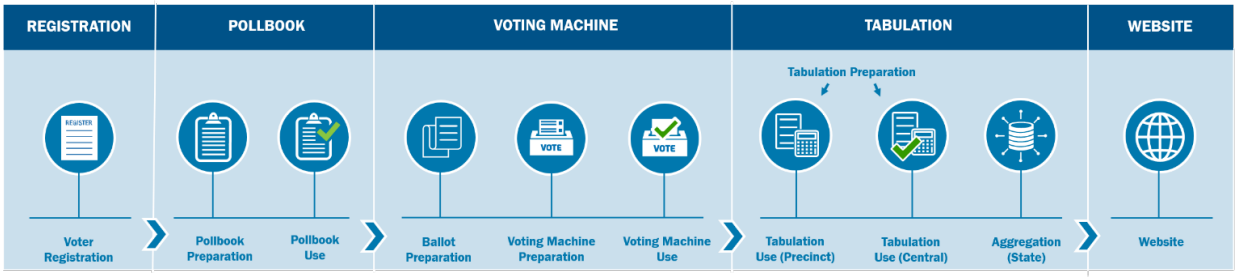

FIGURE 1—ELECTION SYSTEM FUNCTIONAL ECOSYSTEM

Election systems use diverse infrastructure and security controls. Even jurisdictions that deploy cybersecurity best practices are potentially vulnerable to attacks from sophisticated cyber actors, such as advanced nation-state actors. Therefore, detection and recovery methods are equally significant as preventative measures.

Cyber attacks on the integrity of state-level voter registration, pollbooks, and election websites, as well as on the preparation of ballots, voting machines, and tabulation systems, have the potential for greatest functional impact to the ability of jurisdictions to conduct elections, based on fault tree analysis[i] of election system components through each phase of the election process. The following election infrastructure represents the systems, networks, and processes most critical to the security, integrity, and resilience of U.S. elections:

- **Voter registration databases** are used to enter, store, and edit voter registration information, such as servers that host the database and online portals that provide access. Voter registration is an ongoing process to create new records, update existing records, and remove outdated records. Voter registration databases receive data automatically and indirectly (i.e. through manual entry) from a variety of sources, including other government agencies (e.g., the Department of Motor Vehicles) and organizations that aid in the registration process (e.g., voter registration campaigns). The databases contain information on whether people are entitled to vote, where they can vote, and on what unique ballot style they will vote, based upon voter geographical placement within multiple layers of political and taxing districts.
- **Electronic and paper pollbooks** contain information on registered voters at polling places, and can be used to register voters where permitted by law. Before use, pollbooks must be prepared by transferring information from the voter registration database. Pollbooks are comprised of both technology and processes to view, edit, and modify voter records. Pollbooks may be either networked or non-networked. Networked pollbooks are electronic pollbooks with a connection to an external

[i] Fault tree analysis is a widely used method in system reliability, maintainability, and safety analysis. It is a deductive procedure used to determine combinations of hardware and software failures and human errors that could cause undesired outcomes at the system level.

database, and may include a direct connection to the voter registration database or a separate server. Non-networked pollbooks are either paper pollbooks or static digital files on computers.

- **Ballot preparation** is the process of overlaying political geographies with the contests and candidates specific to each district, and then translating those layouts into unique combinations of ballot data. Ballot preparation data takes multiple forms such as ballot images (both paper and electronic), the data files necessary to build ballot images, audio files for special use ballots, and specific files for export to external systems such as websites or Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)-focused digital systems. Ballot preparation also generates the data necessary for tabulating votes within a voting machine, and aggregating tabulated votes within a jurisdiction or state. This process is usually completed in an election management system.
- **Voting machine systems** consist of the technology and processes used to cast and, in some cases, generate voter ballots of all types (paper-based systems, and electronic-based systems like ballot marking devices and direct-recording electronic machines with or without a voter-verified paper audit trail). Voting machines encompass both technology and processes used by election officials to prepare voting machines for ballot tabulation, and in some cases presentation. Specifically, this includes loading the ballot files created during ballot preparation onto voting machines. Voting machines are held in storage in the custody of election officials, but after delivery are placed at voting locations for use during early voting and on Election Day. Voting machines are the most visible form of technology that voters interact with during the voting process.
- Centralized **vote tabulation and aggregation systems** are used to tally votes shared by sub-jurisdictions such as counties, precincts, and in some cases individual machines or even individual ballots. These systems collect and process data to determine the result of an election contest. Tabulation encompasses both technology and processes used to count votes and aggregate results. Vote tabulation processes include hand counting, optical scans of paper ballots, and direct electronic tabulation. Vote tabulation may occur at the precinct-level in addition to centralized tabulation.
- **Official websites** are used by election officials to communicate information to the public, including how to register to vote, where to vote (e.g., precinct look-up tools), and to convey election results (e.g., election night reporting systems). Sometimes election websites are hosted on government-owned infrastructure, but are often hosted by commercial partners.
- **Storage facilities**, which may be located on public or private property, and may be used to store election and voting system infrastructure before Election Day.
- **Polling places** (including early voting locations) are locations where individuals cast their votes and may be physically located on public or private property.
- **Election offices** are locations where election officials conduct official business, including shared workspaces such as public libraries, municipal buildings, private homes, and public areas for jurisdictions without a dedicated workspace.

ELECTION INFRASTRUCTURE CYBER ATTACK CONSEQUENCES

Analysis determined that cyber attacks on each component of the election infrastructure ecosystem may have differing consequences, based on type of cyber impact and the specific targeted election system component. This assessment used the Confidentiality-Integrity-Availability (CIA) Triad information security model[ii] to analyze three types of cyber attacks:

- Confidentiality Attacks, the theft of information;
- Integrity Attacks, the changing of either the information within or the functionality of a system; and
- Availability Attacks, the disruption or denial of the use of the system.

[ii] (U) For more information on the CIA triad, refer to: Center for Internet Security, "EI-ISAC Cybersecurity Spotlight – CIA Triad," 2019, https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/. Accessed July 28, 2020.

Risks can also differ for the same component during preparation and during use (e.g., voting machines may be more accessible to cyber attacks during preparation than on Election Day). Additionally, a successful cyber attack on a voting machine could also cascade onto a tabulation or aggregation system if malware is transferred after voting is complete.

Table 1 provides a high-level overview of the potential consequence of a successful cyber attack by system component. This table does not directly address cyber attacks aimed at undermining public confidence in elections, though the three types of attacks could have a primary or secondary goal of undermining confidence.

TABLE 1—POTENTIAL CONSEQUENCE OF AN ELECTION CYBER ATTACK BY COMPONENT

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Voter Registration	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
Pollbook Preparation	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
Ballot Preparation	Expose Ballot Information	Change Ballot Information During Preparation	Prevent Ballot Preparation
Voting Machine Preparation	Change Voting Machine Functionality to Expose Voter Choices	Change Voting Machine Functionality (Presentation of Ballot/Recording of Choices)	Prevent Voting Machine Functionality
Tabulation Preparation	Change Tabulation Machine Functionality to Expose Results	Change Tabulation Machine Functionality	Prevent Tabulation Machine Functionality
Pollbook Use	Expose Non-public Voter Registration Information	Change Voter Registration Information (In Pollbook)	Prevent Access to Voter Registration Information
Voting Machine Use	Expose Voter Choices	Change Voting Machine Functionality	Prevent Voting Machine Functionality
Tabulation (Precinct)	Expose Tabulation Results Before Intended	Change Results of Vote Tabulation	Prevent Vote Tabulation
Tabulation (Central)	Expose Tabulation Results Before Intended (Aggregation)	Change Results of Vote Tabulation (Aggregation)	Prevent Vote Tabulation (Aggregation)
Aggregation (State)	Expose Aggregation Results Before Intended	Change Results of Vote Aggregation	Prevent Vote Aggregation
Website	Expose Information Not Intended for Public Disclosure	Change Reported Results	Prevent Reporting of Results

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Website	Expose Information Not Intended for Public Disclosure	Change Voter Registration and Precinct Information (In Voter Lookup)	Prevent Voter Lookup of Registration and Precinct Information

JOINT ELECTION INFRASTRUCTURE AND DISINFORMATION ATTACKS

Foreign state and non-state actors leverage information activities as part of broad campaigns to sow discord, manipulate public discourse, and discredit the electoral system to undermine pillars of democracy. In the context of elections, foreign entities aim to:

- Dissuade target audiences from participating in the electoral process through content that suggests their votes do not matter, that abstaining from voting is the most democratic action, or through content that misleads voters about the process of voting.
- Impact candidate selection through, among other activities, pushing fabricated and favorable content about preferred candidates, and fabricated or disparaging content about disfavored candidates.
- Damage the public perception of a fair and free election by pushing false or misleading content regarding election processes and results.

These disinformation campaigns, conducted in concert with cyber attacks on election infrastructure, can amplify disruptions of electoral processes and public distrust of election results. Unauthorized network access allows for surveillance and reconnaissance, and provides opportunities for destructive cyber attacks. Stolen or falsified information can be strategically leaked to shape false narratives. Hijacking online personas and the defacement or alteration of public-facing sites can be leveraged to influence public opinion. The targeting of government systems (even without compromise) can be used to form narratives leading to distrust of the government as stewards of citizen information.

ELECTION INFRASTRUCTURE RISK CRITERIA

Based on these consequences, the assessment applied multiple criteria that assess the scale of cyber risk associated with election infrastructure. The potential scale of an election infrastructure cyber attack is based on factors including whether the infrastructure is being prepared for use or is in use, whether infrastructure technology is networked, and the degree to which infrastructure components are centralized. Risk criteria considerations are not mutually exclusive.

CISA also assesses additional risk criteria related to voter registration, voting machines, and electronic submission of ballots.

Attack Scale: System Preparation

The potential scale of a cyber attack on election infrastructure will be more widespread if a cyber attack occurs during the preparation or programming of election infrastructure versus during its immediate use. While an integrity cyber attack on a single voting machine in a precinct would affect that machine or precinct, cyber attacks on a jurisdiction's central preparation or programming of machines may affect the entire jurisdiction using those machines. If preparation of machines is conducted at the state level, cyber attacks on the preparation process have the potential to impact an entire state. This is true for a single election. However, malware inserted into a single machine during use could propagate to the tabulation and preparations system,

and to all machines in future elections if jurisdictions do not follow best practices for using secure election software system builds.

During system preparation, election jurisdictions rely on files from external sources, such as registration databases, voting system vendors, ballot printers, or ballot programmers. Importing data from external sources raises risk, since sources may use internet connected systems that do not follow cybersecurity best practices. Additionally, an external source may present a cyber attack vector against a wide variety of election jurisdictions if a single source services multiple jurisdictions or states.

Attack Scale: System Networking

The scale of a cyber attack on election infrastructure has the potential to be more widespread if an attack compromises networked infrastructure. For example, electronic pollbooks in some jurisdictions are networked together across the jurisdiction to facilitate vote center operation, whereas electronic pollbooks in other jurisdictions are non-networked. A cyber attack on an individual non-networked pollbook has less chance to spread if the machine remains isolated from a network. An integrity attack on a networked e-pollbook has the potential to affect an entire jurisdiction, while an integrity attack on a local, non-networked pollbook can be isolated to that particular voting location.

Because of that, we assess network connectivity for voting systems to be high risk. Creating and maintaining an airgap for critical systems, such as the vote casting or vote tabulation systems, is a best practice.[iii]

Attack Scale: Centralization

The potential scale of a cyber attack will be more widespread if an attack targets a centralized process versus a localized process. Some jurisdictions tabulate votes at each polling location before aggregating results at a central location, while others only tabulate votes at a central location. An integrity attack on central tabulation systems or processes has the potential for a broader reach than an integrity attack on local tabulation process.

Table 2 provides a brief summary of criteria used to assess cyber risk associated with the potential scale of an election-related cyber attack, assessed by an election infrastructure component. We categorize the scale of an attack into one of three categories:

- Low: Affecting a subset of a jurisdiction
- Medium: Affecting an entire jurisdiction
- High: Affecting an entire state or multiple jurisdictions

For a more detailed look at cyber risk by component, refer to “Table 3—Election Infrastructure Risk Prioritization Matrix” on page 10.

[iii] An airgap is a physical separation between systems that requires data to be moved by some external, manual procedure.

TABLE 2—POTENTIAL SCALE OF AN ELECTION CYBER ATTACK BY COMPONENT

ELECTION COMPONENT	ATTACK VECTOR	SCALE
Voter Registration	Jurisdiction Registration Database	Medium
Voter Registration	State Registration Database	Heavy
Pollbook	Jurisdiction Pollbook Preparation	Medium
Pollbook	State Pollbook Preparation	Heavy
Pollbook	Non-Networked Pollbook Use	Low
Pollbook	Jurisdiction Networked Pollbook Use	Medium
Pollbook	State Networked Pollbook Use	Heavy
Ballot Preparation	Jurisdiction Ballot Preparation	Medium
Ballot Preparation	State Ballot Preparation	Heavy
Voting Machine	Jurisdiction Voting Machine Preparation	Medium
Voting Machine	State Voting Machine Preparation	Heavy
Voting Machine	Voting Machine Use	Low
Tabulation	Tabulation Preparation	Medium
Tabulation	Precinct Tabulation Use	Low
Tabulation	Central Tabulation Use	Medium
Tabulation	State Aggregation	Heavy

ELECTION COMPONENT	ATTACKER VECTOR	SCALE
Website	Jurisdiction Website	Medium
Website	State Website	Heavy

Number of Registered Voters

Electoral jurisdictions vary greatly in size, with some having as few as 100 voters to the largest encompassing several million voters.[2] Jurisdictions with more registered voters manage more risk than jurisdictions with smaller voter populations. The number of registered voters represents the number of individuals in each jurisdiction who could have personal information exposed during a confidentiality attack or experience disruptions at polling places as a result of cyber attacks, or election-related cascading impacts from physical incidents.

Voter Registration System Configuration

States manage their voter registration systems in three primary ways.[3] States with top-down voter registration system host data on a single, central platform of hardware, which is maintained by the state with data and information supplied by local jurisdictions. Bottom-up systems feature data hosted on local hardware and periodically compiled to form a statewide voter registration list. Hybrid systems are a combination of top-down and bottom-up characteristics. As of 2018, 39 states and territories have voter registration systems that are top-down configurations.[4]

States with top-down voter registration systems present attackers with a single system that, if compromised, could disrupt the voting process at a broader scale than jurisdiction-level systems. Since top-down voter registration systems maintain the entire voter registration database for a state, they present a single target for attack that could disrupt many more voters. A bottom-up or hybrid system would require the compromise of a diverse number of systems across a state to achieve similar results. However, cyber and physical security of top-down systems is more likely to be stronger than bottom-up or hybrid systems, based on a review of overall state and local cybersecurity resources and support.

Online Voter Registration

Online voter registration allows residents to complete voter registration forms online. Forty states and territories offer an online voter registration portal in which individuals can register on their own without having to submit a paper form.[5]

Online voter registration systems provide an additional point of vulnerability to enable cyber actors to gain access to voter registration databases and conduct confidentiality, integrity, or availability attacks.[6] Hackers, including nation-state actors, have exploited voter databases in the past to gain illicit access to voter information.[7]

Measures such as same day registration[iv] and provisional ballots are likely to reduce impact of integrity attacks to voter registration systems by providing a fail-safe mechanism to allow eligible voters to correct tampered or deleted data and vote using established processes. Help America Vote Act-required provisional ballot

[iv] Same day registration is the procedure for individuals to register to vote and cast a ballot on the same day. According to the U.S. Election Assistance Commission Election Administration and Voting Survey, 26 states have some form of same day registration, as of 2018.

processes[v] also provided a fail-safe measure of resilience. Even though same-day registration and provisional ballots can provide resiliency, both have the potential to cause disruptions at polling places due to longer processing times that can be required to administer provisional ballots (approximately 15 percent longer than that of normal ballot processes, depending upon the specific processes election officials deploy). Additionally, many election officials believe the best implementation of same-day registration utilizes network connected technology, such as electronic pollbooks, introducing system networking risks, as discussed above.

Voting Machines Without Voter Verified Auditable Paper Record

Direct-recording electronic voting machines capture voting data directly into electronic memory.[8] Many direct-recording electronic voting machines come equipped with a voter-verified paper audit trail feature that provides a printout, verifiable by voters, to ensure their votes are correctly captured. Since 2016, many election officials across the country replaced systems that do not have a voter verified auditable paper record with voting systems that do. Based on research, CISA estimates that greater than 90 percent of cast ballots in 2020 will have a corresponding auditable record.

We assess voting systems without a voter verified auditable paper record as presenting additional risk, based on analysis of the difficulty of identifying electronic manipulation to ensure election integrity in the event of a cyber attack. The existence of a voter verified auditable paper record is the first step in building resiliency, as it can provide the ability for election officials to verify that the outcomes of the election are correct regardless of whether an undetected error or fault in the voting system occurs. However, to provide voters high assurance that errors will be detected, election officials must also conduct regular audits of their elections.

Logic and accuracy testing measures such as parallel monitoring[vi] and hash checks[vii] to ensure software integrity against certified software builds are likely to improve the detection and recovery capability of election officials with regard to their voting systems; especially those without a record that cannot be otherwise audited, though neither measure can replace the use of paper backups to identify irregularities and reduce risk.

Uniformed and Overseas Citizens Absentee Voting Act Electronic Ballots

Certain groups of voters, particularly military and overseas voters, face challenges voting both in-person or through the mail. All jurisdictions are required to offer electronic ballot delivery, per federal law. Many state and local election officials additionally make use of email, fax, and web portals to aid in ballot return for these groups.[9,10] Thirty-one states[viii] and the District of Columbia (D.C.) allow voters covered by the Uniformed and Overseas Citizens Absentee Voting Act to submit their ballots by at least one electronic means, such as internet portal, email, or fax.[11] Five states (Arizona, Colorado, Missouri, North Dakota, and West Virginia) allow Uniformed and Overseas Citizens Absentee Voting Act voters to return ballots using a web-based portal or application. Additionally, several counties within Utah, Colorado, and Oregon conducted a pilot using a mobile voting application and are determining its use moving forward.[12] West Virginia used a similar application in previous elections. Nineteen states[ix] and D.C. allow some voters to return ballots via email or fax, while seven states[x] allow some voters to return ballots via only fax.

---

[v] Provisional ballot processes, or provisional voting, maintains the individual's intent to vote until election officials determine the eligibility status of the individual to cast a ballot in the election. All states except for Minnesota, New Hampshire, and North Dakota issue provisional ballots to individuals on election day, per Section 302 of the Help America Vote Act.

[vi] Parallel monitoring is the process of testing a set of randomly selected voting machines to be tested in election mode during the voting period. The intent is to try to "trick" the system into thinking that it is in a voting location and being used live in the election. Parallel testing could then detect if malicious software had been deployed to only take effect in a specific mode (i.e. Election Mode) or during a specified time (i.e. on Election Day).

[vii] Hash checks are useful to verify data integrity and are conducted by comparing the hash value of received data to the hash value of data as it was sent to detect whether data was altered.

[viii] The 31 states are: Alaska, Arizona, California, Colorado, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Texas, Utah, Washington, and West Virginia.

[ix] The 19 states are: Delaware, Hawaii, Idaho, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, Oregon, South Carolina, Utah, and Washington.

[x] The seven states are: Alaska, California, Florida, Louisiana, Oklahoma, Rhode Island and Texas.

We assess electronic ballot return as presenting additional risk, whether through email, fax, web portal, or mobile application, based on the difficulty of securing the electronic transmission of data. Ballots submitted through electronic means are subject to increased potential to disruption, manipulation, or exposure.

Risks to electronic ballot return are similar to mail-in ballots, but with the potential to impact a higher number of ballots. For example, a man-in-the-middle attack on a physical mail-in ballot requires physical access, and attack scale is limited through proper chain of custody procedures. In contrast, a malicious cyber actor can conduct a man-in-the-middle attack on electronic ballots at a higher scale from a wide range of global locations.

ELECTION INFRASTRUCTURE RISK PRIORITIZATION MATRIX

CISA NRMC assesses differing relative aggregate cyber risk per election infrastructure component, based on fault tree analysis. The prioritization matrix below is calculated based on the technical capability required to conduct a cyber attack,[xi] the potential scale of impact of a cyber attack, and an importance score[xii] to provide a view of risk across election system components. Since election system implementations vary widely among jurisdictions, CISA NRMC evaluated both a "best-case" and "worst-case" system implementation for each election component. This view of "best-case" and "worst-case" impacts the technical capability required to attack each component, but does not alter the attack scale or importance.

Table 3 provides a detailed look at the relative cyber risk to election components in best case (most secure) and worst case (most vulnerable) system implementation, assessed by component and cyber attack type. The table represents the change in risk rating when implementing recommended security controls rather than low security controls. For election infrastructure systems implementing low levels of security controls, we assess nearly any capable threat actor may possess the ability to conduct successful attacks on election infrastructure systems. In contrast, implementing recommended security controls on election infrastructure significantly lowers risk of a successful cyber attack. Some components, even with recommended security controls implemented, represent higher risk to availability attacks as detailed in the below table.

TABLE 3—ELECTION INFRASTRUCTURE RISK PRIORITIZATION MATRIX

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Jurisdiction Registration Database	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Registration Database	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Registration Database	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low

[xi] The technical capability was determined based on the relative difficulty of an attack on the component.
[xii] The importance score was determined based on aggregate importance scale measures assigned by an expert group of elections officials and technology providers.

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
State Registration Database	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Registration Database	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Registration Database	Availability	High	Tier 3 Actor	Heavy	Tier 2 Actor	Medium
Jurisdiction Pollbook Preparation	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Pollbook Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Pollbook Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Pollbook Preparation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Pollbook Preparation	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Medium
State Pollbook Preparation	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Medium
Non-Networked Pollbook Use	Confidentiality	Low	Tier 3 Actor	Low	Tier 1 Actor	Low

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Non-Networked Pollbook Use	Integrity	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Non-Networked Pollbook Use	Availability	Low	Tier 3 Actor	Low	Tier 2 Actor	Low
Jurisdiction Networked Pollbook Use	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Networked Pollbook Use	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Networked Pollbook Use	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Networked Pollbook Use	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Networked Pollbook Use	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Networked Pollbook Use	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Medium
Jurisdiction Pollbook Preparation	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Pollbook Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Jurisdiction Pollbook Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Ballot Preparation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Ballot Preparation	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Ballot Preparation	Availability	High	Tier 3 Actor	Heavy	Tier 2 Actor	Medium
Jurisdiction Voting Machine Preparation	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Voting Machine Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Voting Machine Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Voting Machine Preparation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Voting Machine Preparation	Integrity	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Voting Machine Preparation	Availability	High	Tier 3 Actor	Heavy	Tier 2 Actor	Medium

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Voting Machine Use	Confidentiality	Low	Tier 3 Actor	Heavy	Tier 1 Actor	Low
Voting Machine Use	Integrity	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Voting Machine Use	Availability	Low	Tier 3 Actor	Low	Tier 2 Actor	Low
Tabulation Preparation	Confidentiality	Medium	Tier 3 Actor	Low	Tier 1 Actor	Low
Tabulation Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Tabulation Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
Precinct Tabulation Use	Confidentiality	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Precinct Tabulation Use	Integrity	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Precinct Tabulation Use	Availability	Low	Tier 3 Actor	Low	Tier 2 Actor	Low
Central Tabulation Use	Confidentiality	Medium	Tier 3 Actor	Low	Tier 1 Actor	Low
Central Tabulation Use	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Central Tabulation Use	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Aggregation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Aggregation	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Aggregation	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Medium
Jurisdiction Website	Confidentiality	Medium	Tier 3 Actor	Low	Tier 1 Actor	Low
Jurisdiction Website	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Website	Availability	Medium	Tier 3 Actor	Low	Tier 2 Actor	Low
State Website	Confidentiality	High	Tier 3 Actor	Low	Tier 1 Actor	Low
State Website	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Website	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Low

ATTACK TYPE
***Confidentiality*: the theft of information**
***Integrity*: the changing of either the information within or the functionality of a system**
***Availability*: the disruption or denial of the use of the system**

ATTACK SCALE
***Low*: Affecting a subset of a jurisdiction**
***Medium:* Affecting an entire jurisdiction**
***High:* Affecting an entire state or multiple jurisdictions**

ATTACKER SKILL- LOW/RECOMMENDED CONTROLS
Each capability score was determined based on the relative difficulty of an attack on the component for worst case and best case implementation of system security controls and indicates the technical capability needed by a threat actor to execute a potentially successful attack.

***Tier 1 Actor*: Most capable threat actors that can discover new vulnerabilities ("zero days"), develop custom exploits and tools, and combine online activities with close physical operations. Tier 1 actors include both nation-state and sophisticated sub-national groups.**

***Tier 2 Actor*: Moderately capable threat actors that can exploit most cyber vulnerabilities with sufficient time and can create custom exploits and tools. Tier 2 actors are largely limited to conducting operations over the Internet, through they can also exploit proximate access (e.g., "wardriving") or lax security policies on removable media.**

***Tier 3 Actor*: Lease sophisticated threat actors that rely on readily-available cyber tools to exploit known vulnerabilities. Tier 3 actors do not create their own exploits or tools, but can find them on the dark-web or in existing tool suites.**

RISK RATING- LOW/RECOMMENDED CONTROLS
Each overall risk rating score was determined for both the worst case and best case implementation of system security controls. Ratings are based on aggregate cyber capability and attach scale measures and assessments by an expert group of elections officials and technology providers.

---

[1] RAND Corporation Homeland Security Operational Analysis Center, "Election System Risk Prioritization Report," August 2019, page 1.
[2] David C. Kimball and Brady Baybeck, "Are All Jurisdictions Equal? Size Disparity in Election Administration," Election Law Journal (Vol. 12, No. 2), 2013, pp.130-145.
[3] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 119.
[4] Ibid.
[5] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 122.
[6] National Conference of State Legislatures, "Online Voter Registration," October 25, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx. Accessed July 28, 2020.
[7] Report of the U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure,* page 22.
[8] Verified Voting Foundation, "Voting Equipment in the United States," 2019, https://www.verifiedvoting.org/resources/voting-equipment/. Accessed July 28, 2020.
[9] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 15.
[10] National Conference of State Legislatures, "Electronic Transmission of Ballots," September 5, 2019. https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Accessed July 28, 2020.
[11] Ibid.
[12] Associated Press, "2 Oregon counties offer vote-by-mobile to overseas voters," 2019, https://apnews.com/8ce0fbc400514f55839fa84fb364d7f4. Accessed July 28, 2020.

The Cybersecurity and Infrastructure Security Agency (CISA), National Risk Management Center (NRMC), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. For more information, contact Central@cisa.gov or visit https://www.cisa.gov/national-risk-management.

PDM 20004