

# Appendix A



## 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.

## 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.<sup>1</sup>

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<sup>1</sup> 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

<sup>1</sup> 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<sup>ii</sup> 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.

---

<sup>ii</sup> (U) For more information on the CIA triad, refer to: Center for Internet Security, “EHSAC 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
<b>Voter Registration</b>	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
<b>Pollbook Preparation</b>	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
<b>Ballot Preparation</b>	Expose Ballot Information	Change Ballot Information During Preparation	Prevent Ballot Preparation
<b>Voting Machine Preparation</b>	Change Voting Machine Functionality to Expose Voter Choices	Change Voting Machine Functionality (Presentation of Ballot/Recording of Choices)	Prevent Voting Machine Functionality
<b>Tabulation Preparation</b>	Change Tabulation Machine Functionality to Expose Results	Change Tabulation Machine Functionality	Prevent Tabulation Machine Functionality
<b>Pollbook Use</b>	Expose Non-public Voter Registration Information	Change Voter Registration Information (In Pollbook)	Prevent Access to Voter Registration Information
<b>Voting Machine Use</b>	Expose Voter Choices	Change Voting Machine Functionality	Prevent Voting Machine Functionality
<b>Tabulation (Precinct)</b>	Expose Tabulation Results Before Intended	Change Results of Vote Tabulation	Prevent Vote Tabulation
<b>Tabulation (Central)</b>	Expose Tabulation Results Before Intended (Aggregation)	Change Results of Vote Tabulation (Aggregation)	Prevent Vote Tabulation (Aggregation)
<b>Aggregation (State)</b>	Expose Aggregation Results Before Intended	Change Results of Vote Aggregation	Prevent Vote Aggregation
<b>Website</b>	Expose Information Not Intended for Public Disclosure	Change Reported Results	Prevent Reporting of Results

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
<b>Website</b>	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.<sup>iii</sup>

### 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.

---

<sup>iii</sup> 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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup>

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.<sup>6</sup> Hackers, including nation-state actors, have exploited voter databases in the past to gain illicit access to voter information.<sup>7</sup>

Measures such as same day registration<sup>iv</sup> 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

<sup>iv</sup> 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<sup>v</sup> 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.<sup>8</sup> 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<sup>vi</sup> and hash checks<sup>vii</sup> 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.<sup>9,10</sup> Thirty-one states<sup>viii</sup> 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.<sup>11</sup> 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.<sup>12</sup> West Virginia used a similar application in previous elections. Nineteen states<sup>ix</sup> and D.C. allow some voters to return ballots via email or fax, while seven states<sup>x</sup> allow some voters to return ballots via only fax.

---

<sup>v</sup> 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.

<sup>vi</sup> 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).

<sup>vii</sup> 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.

<sup>viii</sup> 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.

<sup>ix</sup> 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.

<sup>x</sup> 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 NRMCM 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,<sup>xi</sup> the potential scale of impact of a cyber attack, and an importance score<sup>xii</sup> to provide a view of risk across election system components. Since election system implementations vary widely among jurisdictions, CISA NRMCM 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	LOW CONTROLS	RECOMMENDED CONTROLS	RECOMMENDED CONTROLS
			ATTACKER SKILL	RISK RATING	ATTACKER SKILL	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

<sup>xi</sup> The technical capability was determined based on the relative difficulty of an attack on the component.

<sup>xii</sup> 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:** Least 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 attack scale measures and assessments by an expert group of elections officials and technology providers.

<sup>1</sup> RAND Corporation Homeland Security Operational Analysis Center, “Election System Risk Prioritization Report,” August 2019, page 1.

<sup>2</sup> 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.

<sup>3</sup> U.S. Election Assistance Commission, “Election Administration and Voting Survey: 2018 Comprehensive Report,” 2018, page 119.

<sup>4</sup> Ibid.

<sup>5</sup> U.S. Election Assistance Commission, “Election Administration and Voting Survey: 2018 Comprehensive Report,” 2018, page 122.

<sup>6</sup> 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.

<sup>7</sup> 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.

<sup>8</sup> Verified Voting Foundation, “Voting Equipment in the United States,” 2019, <https://www.verifiedvoting.org/resources/voting-equipment/>. Accessed July 28, 2020.

<sup>9</sup> U.S. Election Assistance Commission, “Election Administration and Voting Survey: 2018 Comprehensive Report,” 2018, page 15.

<sup>10</sup> 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.

<sup>11</sup> Ibid.

<sup>12</sup> 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](mailto:Central@cisa.gov) or visit <https://www.cisa.gov/national-risk-management>.



## The Office of Secretary of State

*Brian P. Kemp*  
SECRETARY OF STATE

December 8, 2016

The Honorable Jeh Johnson  
Secretary of Homeland Security  
Department of Homeland Security  
Washington, D.C. 20528

Secretary Johnson,

On November 15, 2016, an IP address associated with the Department of Homeland Security made an unsuccessful attempt to penetrate the Georgia Secretary of State's firewall. I am writing you to ask whether DHS was aware of this attempt and, if so, why DHS was attempting to breach our firewall.

The private-sector security provider that monitors the agency's firewall detected a large unblocked scan event on November 15 at 8:43 AM. The event was an IP address (216.81.81.80) attempting to scan certain aspects of the Georgia Secretary of State's infrastructure. The attempt to breach our system was unsuccessful.

At no time has my office agreed to or permitted DHS to conduct penetration testing or security scans of our network. Moreover, your Department has not contacted my office since this unsuccessful incident to alert us of any security event that would require testing or scanning of our network. This is especially odd and concerning since I serve on the Election Cyber Security Working Group that your office created.

As you may know, the Georgia Secretary of State's office maintains the statewide voter registration database containing the personal information of over 6.5 million Georgians. In addition, we hold the information for over 800,000 corporate entities and over 500,000 licensed or registered professionals.

As Georgia's Secretary of State, I take cyber security very seriously. That is why I have contracted with a global leader in monitored security services to provide immediate responses to these types of threats. This firm analyzes more than 180 billion events a day globally across a 5,000+ customer base which includes many Fortune 500 companies. Clearly, this type of resource and service is necessary to protect Georgians' data against the type of event that occurred on November 15.

Georgia was one of the only few states that did not seek DHS assistance with cyber hygiene scans or penetration testing before this year's election. We declined this assistance due to having already implemented the security measures suggested by DHS. Under 18 U.S.C. § 1030, attempting to gain access or exceeding authorized access to protected computer systems is illegal. Given all these facts, a number of very important questions have been raised that deserve your attention:

1. Did your Department in fact conduct this unauthorized scan?
2. If so, who on your staff authorized this scan?
3. Did your Department conduct this type of scan against any other states' systems without authorization?
4. If so, which states were scanned by DHS without authorization?

I am very concerned by these facts provided by our security services provider, as they raise very serious questions. I would appreciate your prompt and thorough response.

Sincerely,



Brian P. Kemp

CC:

The Honorable Johnny Isakson  
United States Senate

The Honorable Rob Woodall  
United States House of Representatives

The Honorable David Perdue  
United States Senate

The Honorable Austin Scott  
United States House of Representatives

The Honorable Buddy Carter  
United States House of Representatives

The Honorable Doug Collins  
United States House of Representatives

The Honorable Sanford Bishop  
United States House of Representatives

The Honorable Jody Hice  
United States House of Representatives

The Honorable Lynn Westmoreland  
United States House of Representatives

The Honorable Barry Loudermilk  
United States House of Representatives

The Honorable Hank Johnson  
United States House of Representatives

The Honorable Rick Allen  
United States House of Representatives

The Honorable John Lewis  
United States House of Representatives

The Honorable David Scott  
United States House of Representatives

The Honorable Tom Price  
United States House of Representatives

The Honorable Tom Graves  
United States House of Representative



Homeland  
Security

December 12, 2016

The Honorable Brian P. Kemp  
Secretary of State  
State of Georgia  
214 State Capitol  
Atlanta, GA 30334

Dear Secretary Kemp:

Thank you for your December 8, 2016 letter. Due to the publicity that your letter has generated, I wanted to respond promptly to you with initial findings.

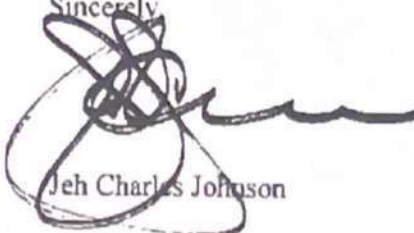
Working with your staff, we have been able to locate, in prompt fashion, the workstation from which the activity that you highlight in your letter occurred. We have reviewed the technical logs and interviewed the user of this computer. The user is a contractor of our Federal Law Enforcement Training Center (FLETC) located in Georgia; he is not a member with our cybersecurity team. We interviewed the contractor and he told us that he accessed your website as part of his normal job duties at FLETC to determine whether incoming FLETC contractors and new employees had a certain type of professional license – a service that, as I understand it, your website provides to the general public. The technical information we have corroborates the contractor's statement, and indicates normal Microsoft Internet Explorer interaction by the contractor's computer with your website.

Most important: there was no scanning of your systems by our cybersecurity experts. As stated before, the contractor using your website is not one of our cybersecurity experts, nor were these inquiries made for the purpose of assessing or determining the security of your website. As we have explained to you and other state election officials, when DHS conducts a cybersecurity scan of a network or system, we do so only with the cooperation and consent of the system owner.



The Honorable Brian P. Kemp  
Page 2

This is an interim response to your inquiry, subject to change. Given the publicity around your inquiry, I wanted to provide this response as soon as possible. We look forward to continue working with you and your team on this matter.

Sincerely,  
  
Jeh Charles Johnson

cc:

The Honorable Johnny Isakson  
United States Senate

The Honorable Rob Woodall  
United States House of Representatives

The Honorable David Perdue  
United States Senate

The Honorable Austin Scott  
United States House of Representatives

The Honorable Buddy Carter  
United States House of Representatives

The Honorable Doug Collins  
United States House of Representatives

The Honorable Sanford Bishop  
United States House of Representatives

The Honorable Jody Hice  
United States House of Representatives

The Honorable Lynn Westmoreland  
United States House of Representatives

The Honorable Barry Loudermilk  
United States House of Representatives

The Honorable Hank Johnson  
United States House of Representatives

The Honorable Rick Allen  
United States House of Representatives

The Honorable John Lewis  
United States House of Representatives

The Honorable David Scott  
United States House of Representatives

The Honorable Tom Price  
United States House of Representatives

The Honorable Tom Graves  
United States House of Representative

ATTACHMENT 4



## The Office of Secretary of State

*Brian P. Kemp*  
SECRETARY OF STATE

December 13, 2016

President-Elect Donald J. Trump  
725 Fifth Avenue  
New York, NY 10022

Dear President-Elect Trump,

I respectfully write today to request that you task your new Secretary of Homeland Security with investigating the failed cyber-attacks against the Georgia Secretary of State's network firewall.

In my letter dated December 8, 2016 to current DHS Secretary Jeh Johnson, I detailed a large attack on our system from November 15, 2016 that traced back to an IP address associated with the Department of Homeland Security.

In addition to this event, my staff has uncovered further instances in 2016 when IP addresses connected to DHS attempted to infiltrate our network. These events were less intrusive scans that did not raise as many red flags. However, the timing is very concerning as these scans correspond to key election dates and times when I was speaking out against DHS' plans to designate elections systems as "critical infrastructure."

The dates in question include the day I testified against DHS' position before the House Oversight Committee; the day of a conference call discussing the designation of Critical Infrastructure with Georgia officials; and several other key election dates, including Election Day. An outline of these attacks are attached to this letter.

Since contacting DHS with these concerns, we have collaborated with the agency and provided extensive, additional information. Last night I received a letter from Secretary Johnson which lacked any specific information as to the attacks' intent or origin despite the fact that many questions remain unanswered.

The people of Georgia are very concerned about what exactly happened here, and they are demanding transparent and honest answers. It appears that will not happen with the current administration. Given that we are a few weeks away from the transition, I write to ask for your help in providing those answers when you assume the Presidency later next month.

Sincerely,

*B.P.K.*  
Brian P. Kemp

### SCANNING ACTIVITIES FROM 2016

Day	Date	Time	Relevance to Timing of Scanning Activity
Tuesday	Feb. 2, 2016	13:03 CST	This scan was conducted the day after Georgia's voter registration deadline for the Presidential Preference Primary.
Sunday	Feb. 28, 2016	13:19 CST	This scan was conducted on a Sunday afternoon, two days before Georgia's Presidential Preference Primary dubbed the SEC Primary.
Monday	May 23, 2016	08:42 CDT	This scan was conducted the day before Georgia's General Primary.
Monday	Sep. 12, 2016	11:52 CDT	This scan was conducted just before a conference call between DHS & GEMA to discuss designating elections systems as critical infrastructure, and only three days after a call between elections officials and Secretary Johnson on designating elections systems critical infrastructure.
Wednesday	Sep. 28, 2016	07:54 CDT	This scan was conducted just hours before my testimony opposing the designation of elections systems as critical infrastructure.
Monday	Oct. 3, 2016	10:41 CDT	This scan was conducted on the Monday after my Congressional testimony opposing the designation of elections systems as critical infrastructure.
Thursday	Oct. 6, 2016	10:14 CDT	This scan was conducted the week after my Congressional testimony opposing the designation of elections systems as critical infrastructure.
Monday	Nov. 7, 2016	12:15 CST	This scan was conducted the day before Election Day.
Tuesday	Nov. 8, 2016	07:35 CST	This scan was conducted on Election Day.
Tuesday	Nov. 15, 2016	07:43 CST	This scan was conducted exactly one week after the General Election, prior to election results being certified.



RON WYDEN  
OREGON

RANKING MEMBER OF COMMITTEE ON  
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING  
WASHINGTON, DC 20510  
(202) 224-5244

United States Senate  
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE

COMMITTEE ON BUDGET

COMMITTEE ON ENERGY & NATURAL RESOURCES

SELECT COMMITTEE ON INTELLIGENCE

JOINT COMMITTEE ON TAXATION

October 3, 2017

Mr. Phillip Braithwaite  
Chief Executive Officer  
Hart InterCivic  
15500 Wells Port Drive  
Austin, TX 78728

Dear Mr. Braithwaite:

I write to seek public answers about cybersecurity threats to our election infrastructure and whether the election technology industry has taken steps to defend against hackers, including those working for foreign governments.

As our election systems have come under unprecedented scrutiny, public faith in the security of our electoral process at every level is more important than ever before. Ensuring that Americans can trust that election systems and infrastructure are secure is necessary to protecting confidence in our electoral process and democratic government.

In order for Congress and the American people to better understand the threats that your company faces and the steps you have taken to protect against them, I would appreciate complete answers to the following questions by October 31, 2017.

1. Does your company employ a Chief Information Security Officer? If yes, to whom do they directly report? If not, why not?
2. How many employees work solely on corporate or product information security?
3. In the last five years, how many times has your company utilized an outside cybersecurity firm to audit the security of your products and conduct penetration tests of your corporate information technology infrastructure?
4. Has your company addressed all of the issues discovered by these cybersecurity experts and implemented all of their recommendations? If not, why not?
5. Do you have a process in place to receive and respond to unsolicited vulnerability reports from cybersecurity researchers and other third parties? How many times in the past five years has your company received such reports?
6. Are you aware of any data breaches or other cybersecurity incidents in which an attacker gained unauthorized access to your internal systems, corporate data or customer data? If your company has suffered one or more data breaches or other cybersecurity incidents, have you reported these incidents to federal, state and local authorities? If not, why not?

911 NE 11TH AVENUE  
SUITE 630  
PORTLAND, OR 97232  
(503) 326-7525

405 EAST 8TH AVE  
SUITE 2020  
EUGENE, OR 97401  
(541) 431-0229

SAC ANNEX BUILDING  
105 FIR ST  
SUITE 201  
LA GRANDE, OR 97850  
(541) 962-7691


U.S. COURTHOUSE  
310 WEST 6TH ST  
ROOM 118  
MEDFORD, OR 97501  
(541) 858-5122

THE JAMISON BUILDING  
131 NW HAWTHORNE AVE  
SUITE 107  
BEND, OR 97701  
(541) 330-9142

707 E 10TH ST, SE  
SUITE 285  
SALEM, OR 97301  
(503) 589-4555

[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)  
PRINTED ON RECYCLED PAPER



- 
7. Has your company implemented the best practices described in the National Institute of Standards and Technology (NIST) 2015 Voluntary Voting Systems Guidelines 1.1? If not, why not?
  8. Has your firm implemented the best practices described in the NIST Cybersecurity Framework 1.0? If not, why not?

If you have any questions about this request, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,



Ron Wyden  
United States Senator

# Congress of the United States

Washington, DC 20510

December 6, 2019

Sami Mnaymneh  
Founder and Co-Chief Executive Officer  
H.I.G. Capital, LLC  
1450 Brickell Avenue 31st Floor  
Miami, FL 33131

Tony Tamer  
Founder and Co-Chief Executive Officer  
H.I.G. Capital, LLC  
1450 Brickell Avenue 31st Floor  
Miami, FL 33131

Dear Messrs. Mnaymneh and Tamer:

We are writing to request information regarding H.I.G. Capital's (H.I.G.) investment in Hart InterCivic Inc. (Hart InterCivic) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.<sup>1</sup> For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"<sup>2</sup> owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimmed on security in favor of convenience," leaving voting systems across the country "prone to security problems."<sup>3</sup> In light of these concerns, we request that you provide information about your firm, the portfolio

<sup>1</sup> Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, <https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/>; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, <https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html>.

<sup>2</sup> ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It," Jessica Huseman, October 28, 2019, <https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it>.

<sup>3</sup> Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, <https://apnews.com/f6876669cb6b4c4c9850844f8e015b4c>.



companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market.<sup>4</sup> Today, three large vendors—Election Systems & Software, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.<sup>5</sup> Private equity firms reportedly own or control each of these vendors, with very limited “information available in the public domain about their operations and financial performance.”<sup>6</sup> While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.<sup>7</sup>

Concentration in the election technology market and the fact that vendors are often “more seasoned in voting machine and technical services contract negotiations” than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.<sup>8</sup> In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider “the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable” when signing contracts, because vendors typically make their profits by ensuring “that they will be around to maintain it after the sale.” The EAC has warned election officials that “[i]f you do not manage the vendors, they will manage you.”<sup>9</sup>

Election security experts have noted for years that our nation’s election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States’ election infrastructure as “critical infrastructure” in order to prioritize the protection of our elections and to more effectively assist state and local election

<sup>4</sup> Bloomberg, “Private Equity Controls the Gatekeepers of American Democracy,” Anders Melin and Reade Pickert, November 3, 2018, <https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy>.

<sup>5</sup> Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

<sup>6</sup> Id.

<sup>7</sup> Id.

<sup>8</sup> Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, [https://www.brennancenter.org/sites/default/files/publications/Americas\\_Voting\\_Machines\\_At\\_Risk.pdf](https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf); Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

<sup>9</sup> U.S. Election Assistance Commission, “Ten Things to Know About Selecting a Voting System,” October 14, 2017, <https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/>.



officials in addressing these risks.<sup>10</sup> However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk.<sup>11</sup> In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state “using some machines that are no longer manufactured.”<sup>12</sup> Moreover, even when state and local officials work on replacing antiquated machines, many continue to “run on old software that will soon be outdated and more vulnerable to hackers.”<sup>13</sup>

In 2018 alone “voters in South Carolina [were] reporting machines that switched their votes after they’d inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana.”<sup>14</sup> In addition, researchers recently uncovered previously undisclosed vulnerabilities in “nearly three dozen backend election systems in 10 states.”<sup>15</sup> And, just this year, after the Democratic candidate’s electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county’s Republican Chairwoman said, “[n]othing went right on Election Day. Everything went wrong. That’s a problem.”<sup>16</sup> These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

H.I.G. reportedly owns or has had investments in Hart InterCivic, a major election technology vendor. In order to help us understand your firm’s role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.<sup>17</sup>
2. Which election technology companies, including all affiliates or related entities, does H.I.G. have a stake in or own? Please provide the name of and a brief description of the services each company provides.

<sup>10</sup> Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” January 6, 2017, <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

<sup>11</sup> AP News, “US election integrity depends on security-challenged firms,” Frank Bajak, October 29, 2018, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

<sup>12</sup> Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, [https://www.brennancenter.org/sites/default/files/publications/Americas\\_Voting\\_Machines\\_At\\_Risk.pdf](https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf).

<sup>13</sup> Associated Press, “AP Exclusive: New election systems use vulnerable software,” Tami Abdollah, July 13, 2019, <https://apnews.com/e5c070c31f3c497fa9e6875f426ccde1>.

<sup>14</sup> Vice, “Here’s Why All the Voting Machines Are Broken and the Lines Are Extremely Long,” Jason Koebler and Matthew Gault, November 6, 2018, [https://www.vice.com/en\\_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long](https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long).

<sup>15</sup> Vice, “Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials,” Kim Zetter, August 8, 2019, [https://www.vice.com/en\\_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials](https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials).

<sup>16</sup> New York Times, “A Pennsylvania Country’s Election Day Nightmare Underscores Voting Machine Concerns,” Nick Corasaniti, November 30, 2019, <https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html>.

<sup>17</sup> Stop Wall Street Looting Act, S.2155, <https://www.congress.gov/bills/116th-congress/senate-bill/2155>.

- a. Which election technology companies, including all affiliates or related entities, has H.I.G. had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.
  - b. For each election technology company H.I.G. had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
    - i. The name of the company
    - ii. Ownership stake
    - iii. Total revenue
    - iv. Net income
    - v. Percentage of revenue dedicated to research and development
    - vi. Total number of employees
    - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
    - viii. Other private-equity firms that own a stake in the company
3. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
4. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
5. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
6. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.




7. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or **breach of contract**? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,



Elizabeth Warren  
United States Senator



Amy Klobuchar  
United States Senator



Ron Wyden  
United States Senator



Mark Pocan  
Member of Congress

JANUARY 29, 2021

# THE SOLARWINDS CYBERATTACK

[f share](#) [t tweet](#) [e email](#) [p print](#)

## KEY TAKEAWAYS

- The SolarWinds computer hack is one of the most sophisticated and large-scale cyber operations ever identified. The U.S. government has stated the operation is an intelligence gathering effort and has attributed it to an actor that is likely Russian in origin.
- The operation has affected federal agencies, courts, numerous private sector companies, and state and local governments across the country.
- It is an example of a digital supply chain attack, in which hackers insert malicious code into trusted third-party software, thus infecting potentially all of the hacked company's customers.

<https://www.cisa.gov/graphics/papers/the-solarwinds-cyberattack>

Page 1 of 8

The SolarWinds computer hack is a serious security issue for the United States. The operation has affected federal agencies, the federal courts, numerous private-sector companies, and state and local governments across the country. It is one of the most sophisticated cyberattacks ever conducted. Only a handful of countries could mount the effort and resources necessary to conduct an operation of this scale, technical sophistication, and apparent objective.

The operation is an example of a digital supply chain attack, in which hackers insert malicious code into trusted third-party software, thus infecting potentially all of the hacked software company's customers. Increasing the cybersecurity of digital supply chains is a top cybersecurity issue facing the 117th Congress, the Biden administration, and American technology companies.

## A DIGITAL TROJAN HORSE

SolarWinds is a company based in Austin, Texas, that provides large-scale information technology infrastructure management software and services to businesses and government agencies. It has more than 320,000 customers in 190 countries, including 499 of the Fortune 500.

In December 2020, FireEye, a cybersecurity consulting firm, uncovered and disclosed what is now called the SolarWinds operation. Hackers inserted malicious code into an update for

<https://www.cisa.gov/graphics/papers/the-solarwinds-cyberattack>

Page 2 of 8

The SolarWinds Cyberattack

8/25/21, 10:22 PM

The SolarWinds Cyberattack

8/25/21, 10:22 PM

SolarWinds' popular network management platform, known as Orion. Customers who routinely updated their Orion software unknowingly downloaded the embedded virus into their systems. Once inside, the attackers could choose which areas to access and were able to move through systems and conduct their operations undetected.

The attackers were meticulous in covering their tracks and took extreme steps to remain undiscovered. While investigations are ongoing, SolarWinds' current understanding is that the operation began in September 2019, when attackers first breached the system. How the attackers gained access is still unknown. The malware was deployed in February 2020, and customers downloaded the Orion update through March and April. By last May, attackers had started to move within the targeted systems, reading emails and other documents. They remained undetected for the next eight months. According to DHS, given the persistence of these attackers, the campaign may be ongoing and other attacks and victims may be identified as the investigation continues.

## SOLARWINDS OPERATION TIMELINE

<https://www.cisa.gov/graphics/papers/the-solarwinds-cyberattack>

Page 3 of 8



On January 5, the FBI, Cybersecurity and Infrastructure Security Agency, Office of the Director of National Intelligence, and National Security Agency released a joint statement saying that their investigation so far indicated "an Advanced Persistent Threat actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort."

The agencies noted that while there were approximately 18,000 private and public sector victims that downloaded the infected Orion software, "a much smaller number have been compromised by follow-on activity on their systems." Government agencies confirmed to be affected by the attack include at least the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Labor, State, and Treasury, as well as the National Institutes of Health. More agencies are likely to be added to the list as investigators learn more about the attack.

<https://www.cisa.gov/graphics/papers/the-solarwinds-cyberattack>

Page 4 of 8

The Department of Justice says it believes the attackers accessed "around 3%" of DOJ email inboxes but not any classified systems. The hackers reportedly breached the email system used by the most senior Treasury Department officials. They also targeted state and local governments and the federal court system. The federal judiciary's electronic case management and filing system was likely compromised as part of the operation. This puts at risk sensitive case records and information that would be of great value to Russian intelligence, including trade secrets, investigative techniques, and information on targets of surveillance operations. Federal courts are currently accepting highly sensitive case documents only in paper form or on secure devices like thumb drives as they respond to the breach.

Data from Microsoft shows that global IT companies, think tanks, non-governmental organizations, and government contractors working for defense and national security organizations appear to have been targeted in the operation. Targeted private-sector companies reportedly include Belkin, Cisco, Deloitte, Intel, Nvidia, and VMware. The head of FireEye has stated that around 50 organizations were "genuinely impacted" by the operation.

The economic damage from the operation is likely to be immense. Some experts estimate it may cost as much as \$100 billion over many months to root out malicious code and ensure systems are not compromised. From an espionage perspective, the damage is impossible to calculate but is likely to be substantial. Federal agencies and global companies may spend years determining whether they were breached, what information was accessed, and what

communications were read. Officials are still trying to understand the exact purpose of the operation and whether there may be more sinister objectives in addition to espionage, such as inserting backdoor access into key government agencies, major IT and cybersecurity companies, critical infrastructure like the electric grid, and nuclear storage facilities. This access may allow the hacker to affect the integrity and availability of these systems, including disrupting essential services.

## THE FEDERAL RESPONSE TO THE OPERATION

The federal government spends billions of dollars each year on cybersecurity. Yet for months, none of the government's defenses, spread across dozens of federal agencies, detected the intrusion. Responding to the attack and strengthening supply chain security is one of the top cybersecurity issues facing the 117th Congress, the Biden administration, and American technology companies.

President Biden's nominees who will lead the response to the operation and formulate U.S. cybersecurity policy have highlighted the urgent threat the attack presents. Alejandro Mayorkas, nominated to head DHS, stated at his confirmation hearing, "the cybersecurity of our nation will be one of my highest priorities because I concur with you that the threat is real, and the threat is every day, and we have to do a better job than we are doing now." Director of National Intelligence Avril Haines cited the asymmetry of the cyber threat as among the greatest that we face in the United States. Secretary of

Defense Lloyd Austin committed to a top-down review of DOD's cyber operations during his confirmation hearing and said of the attack, "Russia should be held accountable."

President Biden has proposed a significant investment in modernizing and securing federal IT as part of the administration's \$1.9 trillion coronavirus relief proposal. It calls for \$9 billion for the Technology Modernization Fund, an existing fund authorized by the Modernizing Government Technology Act of 2017. The fund received \$100 million in fiscal year 2018 and \$25 million in fiscal years 2019 and 2020.

The Cybersecurity and Infrastructure Security Agency and the national cyber director – a new position Congress created in the fiscal year 2021 National Defense Authorization Act – will play key roles in responding to the attack and developing policies to improve the nation's cybersecurity. U.S. Comptroller General Gene Dodaro highlighted the role of the national cyber director in a recent RPC interview, saying, "it will be especially critical to fill this position and to ensure that the director has the authorities and capabilities necessary to (1) ensure that federal entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and (2) coordinate the government's efforts to overcome the nation's cyber-related threats and challenges."

Senator Rubio, the top Republican on the Intelligence Committee, has called the operation "a grave risk to federal, to state, to local governments, to critical infrastructure, to the private sector" and said, "America must retaliate." Senator Warner, the committee's top

Democrat, has said Congress will reexamine whether there should be a national data breach notification requirement. Senators Wicker, Thune, and Moran released a joint statement after receiving a briefing from the Commerce Department on the operation: "Cyberattacks by nation states like Russia and China threaten our economy and national security. Our response should be swift and clear." Senators Portman and Peters announced that the Homeland Security and Governmental Affairs Committee would hold hearings on the attack and work on "bipartisan comprehensive cybersecurity legislation."

The Government Accountability Office has conducted oversight of cybersecurity and provided federal agencies numerous recommendations to better manage supply chain risk. Other policy options for Congress include: reviewing CISA's authorities and resources; increasing sharing and analysis of threat intelligence between the public and private sectors; strengthening and establishing international rules and norms in cyberspace; oversight of DHS, the FBI, NSA, U.S. Cyber Command, the Commerce Department, and other agencies; and taking steps to hold other countries accountable for cyberattacks, whether through sanctions or other means.

ISSUE TAG: TECHNOLOGY