KONRAD ADENAUER STIFTUNG

An Agenda for U.S. Election Cybersecurity

William T. Adler and Mallory Knodel
Center for Democracy and Technology

CENTER FOR DEMOCRACY & TECHNOLOGY

FEBRUARY 2021

www.kas.de

The Center for Democracy & Technology (CDT) is a non-partisan, non-profit U.S.-based civil society organization that works globally to defend human rights and civil liberties online. For 25 years CDT has played a leading role in shaping the policies, practices, and norms that have empowered individuals to more effectively use the internet as speakers, entrepreneurs, and active citizens. CDT brings legal and technical expertise, thought leadership, and coalition-building skills to its work with domestic and global policy institutions, regulators, standards bodies, governance organizations, and courts.

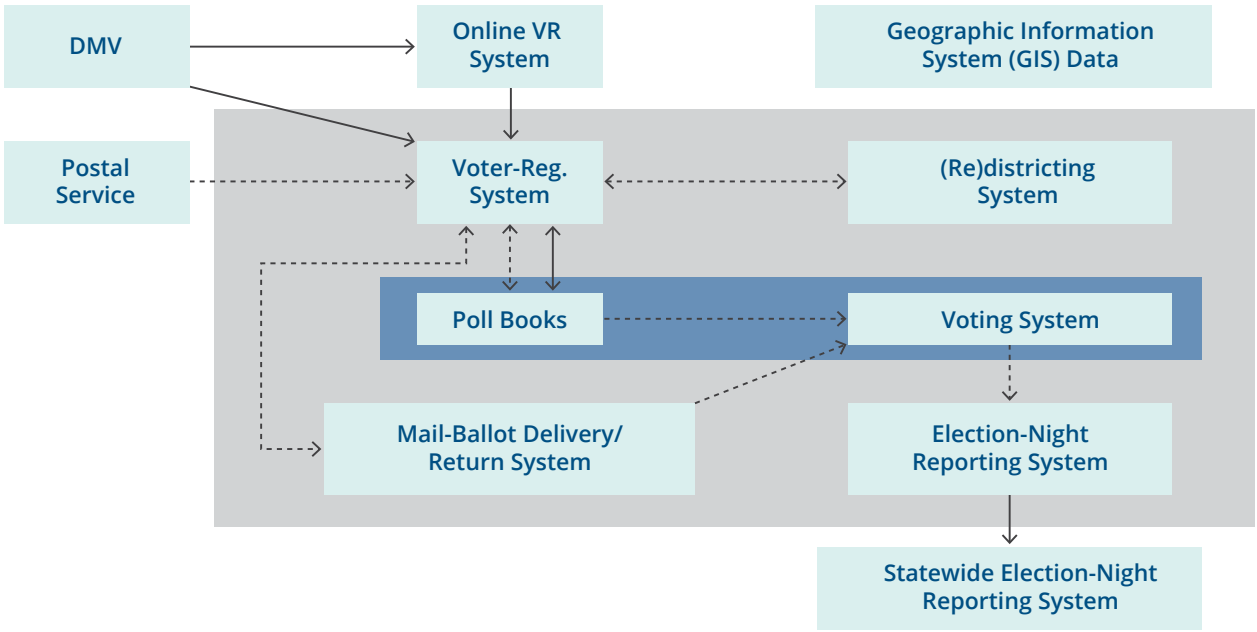
At CDT, we work to preserve the user-controlled nature of the internet and champion freedom of expression. In the United States, voting is one of the ways in which citizens choose how their voices are represented in government. That is why protecting the election process is critical to the functioning of our democracy. CDT works to promote the use of technology in ways that preserve and expand access to the vote, which includes ensuring that elections are secure and auditable.

Table of Contents

Introduction: U.S. democracy in the digital age

Although no election is flawless, a functioning democratic government rests on the people's trust in electoral systems to produce fair and accurate results. Yet, during political campaigns, and before, during and after the elections themselves, malicious actors can influence information flows; public opinion is often manufactured and manipulated; and digital and analogue election infrastructure continue to have weaknesses. Policymakers can support the work of election officials to ensure that the elections are fair, secure, and efficient, that voters have the ability to cast their vote without obstacle and, most importantly, that every vote is counted as intended.

This year, the COVID-19 pandemic posed an extra challenge for election officials. But even without a pandemic, election administration is more complicated than it might seem at first glance. The following graphic, reproduced from election administration expert Charles Stewart III, depicts the components of election infrastructure and the paths by which information flows between them:



Arrows depict the direction of information flow between component systems. Solid lines indicate flows that typically rely on the Internet or other networks that are connected to the Internet; dashed lines indicate information flows that typically are "air-locked" from outside networks. The dark blue box indicates systems that are typically deployed in individual polling places; the grey box indicates systems that are typically centralized in a local jurisdiction's election office.

Reproduced from Stewart III, Charles. "The 2016 U.S. Election: Fears and Facts About Electoral Integrity." Journal of Democracy 28:2 (2017), p. 56, Figure 2. © 2017 National Endowment for Democracy. Reprinted with permission of Johns Hopkins University Press.

Source: This schematic of voting information-system architecture is based on the work of Merle King. For King's full schematic, see https://www.nist.gov/system/files/documents/itl/vote/tgdc-feb-2016-day1-merle-king.pdf#page=14.

It is critical to secure these connections and transmissions, especially those across the open internet, which are represented by solid lines in the figure. A cyber attack, ranging from data capture to manipulation, is possible any time information is transmitted over the internet. It is also critical to physically secure even the "air-gapped" components that are not connected to the internet. There are known security flaws with many components and machines still in use that could enable a hacker with physical access to change the software on a machine.

One challenge to secure elections is that responsibility for components of election infrastructure are spread across a large number of jurisdictions and authorities. The federal government sets some minimum standards for election machinery and operations and provides some guidance and assistance. States maintain voter registration databases and statewide results reporting systems. But counties and localities are responsible for running the elections themselves: checking people in, administering in-person voting infrastructure, and tallying votes. This creates the possibility for diffusion of responsibility, making security dependent on good communication across federal, state, and local levels. Fortunately, there have been significant improvements in coordination in recent years.

Improvements to security are not only about ensuring that components cannot be tampered with, but also about improving trust. Even with no evidence of major problems in the 2020 general election, and with a coalition of election officials releasing a statement saying that the election "was the most secure in American history," the weeks following the election were marked by rampant disinformation campaigns about alleged but unproven insecurities in the electoral process. This clearly demonstrates that there is work to be done not only to secure elections but to convince the public that elections, and election results, can be trusted. This involves making real improvements to cybersecurity and electoral processes, as well as engaging in voter education about how elections work and what safeguards exist to secure them.

For this report, we explore the challenges of maintaining security in U.S. elections and how election officials and policymakers might best address them. We examine the vulnerabilities in various components of the election infrastructure used in the biennial national elections. We analyze an array of events and situations that arose in recent elections including those in 2020, and we offer best practices for a U.S. elections cybersecurity agenda. While focused on American elections, we hope that some of the findings here can also provide guidance for other countries with different election infrastructures and needs.

Who has authority over American elections?

The constitutional framework divides authority between Congress and the states

The U.S. does not have a single, unified electoral system. Rather, the U.S. Constitution creates a role for both states and Congress in determining how elections for federal office (i.e., president, vice president, and members of the U.S. Congress) are administered. The Elections Clause of the Constitution states, in part:

> *The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations.*

The Constitution also says that "each State shall appoint, in such Manner as the Legislature thereof may direct," electors to the Electoral College that will elect the president.

So, although Congress has the ability to set standards and rules—and indeed it has passed major legislation regarding voter registration, accessibility, and racial discrimination—the states are given broad discretion to set state-specific rules and procedures for all aspects of election administration not specified by Congress. In response to the COVID-19 pandemic of 2020, for example, many states used this authority to make it easier for voters to vote by mail.

States largely delegate election administration to smaller jurisdictions

In most states, responsibility to administer the elections themselves is delegated to counties, cities, and towns. Accordingly, across the country, there are about 8,000 jurisdictions responsible for elections. That can include the purchasing and operating of hardware, software, equipment and, to a large extent, maintaining the security of those assets. The population of these jurisdictions can range from just a few hundred registered voters to nearly 5 million in the largest election jurisdiction, Los Angeles County, California.

A comprehensive 2018 report identified the decentralized U.S. elections system as a major factor exacerbating cybersecurity concerns, noting: "Because the U.S. elections system is highly decentralized, responsibility for cybersecurity often falls to the county or municipal level where expertise and resources may be quite limited." This challenge may also be amplified by the sheer

number of elections, which is partly due to public participation in party primaries, and partly due to the high number of elected offices—by one estimate, there are over half a million elected officials in the U.S.

The federal government plays a largely assistive role

Voluntary Voting System Guidelines

In 2000, the general election for President hinged on just a few hundred votes in Florida, exposing numerous problems with Florida's voting machines, procedures, and America's patchwork election infrastructure. In the aftermath of the election, with unprecedented national attention focused on election administration, Congress passed the Help America Vote Act (HAVA) of 2002, a package of election infrastructure improvements. HAVA created new and fairly basic minimum standards, such as the requirement that states provide voters with "fail safe" provisional ballots. It also provided funding for replacement of obsolete voting machines. Importantly, it created the Election Assistance Commission (EAC), a clearinghouse for election administration with responsibilities such as disbursing of funding, developing Voluntary Voting System Guidelines (VVSG), and conducting and publishing original research.

Broadly speaking, the VVSG, which were first adopted by the EAC in 2005, define best practices with the equipment used to define, cast, and count ballots. The EAC also uses the VVSG to certify specific systems. States and territories set standards for their voting systems that can be based on requirements in the VVSG, or EAC certification. But following VVSG guidance is optional; indeed, several states and territories do not refer to the VVSG or EAC certification in their standards. And when states do set standards, much responsibility is left to the smaller jurisdictions to comply with those standards. With such a patchwork system, there are many opportunities for security vulnerabilities.

The EAC is currently considering a revised set of guidance—"VVSG 2.0"— which re-organizes, updates, and expands the guidelines.

"Critical infrastructure" designation

After Russian hackers targeted U.S. election infrastructure in 2016, the federal government has played an increasingly prominent facilitatory and coordinating role in improving election cybersecurity.

In January 2017, the Department of Homeland Security (DHS) designated election infrastructure (referring to "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments") as "critical infrastructure." The federal government uses the "critical infrastructure" designation to indicate "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The critical infrastructure designation has both international and domestic consequences. Internationally, it enables the federal government to take action against foreign actors who tamper with elections. It also brings election infrastructure under a 2015 United Nations nonbinding consensus report establishing norms around protecting critical infrastructure from cyberattack, and not attacking other nations' critical infrastructure. Domestically, it raised the priority for DHS to provide security assistance to state and local election jurisdictions, and enabled DHS to establish formal mechanisms for providing election security-related information, training, and other tools across federal, state, and local entities.

Notably, the designation sets the Cybersecurity and Infrastructure Agency (CISA), an agency established within DHS in November 2018, as the federal entity responsible for coordinating efforts to protect election infrastructure. CISA has since provided free security services and assessments to election officials across the country, the most popular being remote penetration testing and vulnerability assessments. CISA also coordinates information sharing on security incidents, from the federal level down to the local level. CISA received praise for its ability to quickly relay information to election officials when Iranian hackers sent a series of intimidating and misleading emails to voters this October—perhaps the highest-profile cybersecurity incident during the 2020 election cycle.

The improvement of federal coordination of election security has generally been considered a success and has been received positively by state election stakeholders. But there are still major improvements to be made to U.S. election infrastructure, especially as we now turn to the complexities of the systems themselves.

Components of election infrastructure

Election infrastructure consists of many systems—computerized and non-computerized—with potentially exploitable security vulnerabilities. We highlight just a few of them here, but refer the reader to "Securing the Vote," a 2018 report by the National Academies of Sciences, Engineering, and Medicine, for a more thorough treatment.

Voter registration

Because voters must be registered in order to vote in the United States, accurate voter rolls are critical for smooth election administration. But voter registration poses unique challenges. In many countries, the government assumes much of the responsibility for maintaining voter rolls. In the U.S., however, individuals shoulder nearly the entire burden of maintaining an active registration. Voters are not automatically registered when they reach voting age, nor is their registration changed when they move. This style of voter registration creates a number of problems:

- **Low turnout.** Coupled with the widespread lack of ability to register to vote at polling places, non-automatic registration likely poses a barrier to turnout.
- **High cost.** A study conducted by the Pew Center on the States found that costs to maintain voter rolls in the U.S. are up to 12 times higher, per active voter, than in Canada, which has a national voter registration system.
- **Inaccuracy.** The Pew study also found that 1 in 8 registrations are inaccurate. There are not always automatic processes for updating the rolls when voters change addresses or die.

Because of their importance, voter registration databases are a high-risk cybersecurity target. Specifically, they can be targets for confidentiality, integrity, and availability attacks.

Much of the content of voter registration databases is public. But they often include potentially valuable confidential information used to identify voters, such as social security numbers and dates of birth. This puts them at risk of a confidentiality attack, which is when attackers obtain information intended to be kept private. The 2019 U.S. Department of Justice report by Special Counsel Robert Mueller shows that Russians gained access to the statewide voter registration database in Illinois:

> *By at least the summer of 2016, [Russian military intelligence agency] GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as 'SQL injection,' by which malicious code was sent to the state or local website*

in order to run commands (such as exfiltrating the database contents). In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections [(SBOE)] by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified.

Another confidentiality attack may have occurred in 2020, when Iranian hackers allegedly obtained confidential voter registration data, including the last 4 digits of voters' social security numbers. In this case, the information was used in a misleading video to spread disinformation about the feasibility of an attack on elections using widespread absentee fraud (see the following section on absentee and mail-in voting for why such an attack is not feasible). The attack ostensibly targeted voters in Alaska and Florida, although details are still not entirely clear.

An integrity attack occurs when an intruder is able to alter data. Such an attack on voter registration data, such as one that removed numerous voters or placed them in the wrong precinct, would result in major problems. For in-person voters, it could produce long lines on election day by forcing people to cast provisional ballots. For absentee voters, it could result in ballots being sent to the wrong addresses, or ballots being rejected due to failed verification checks. In a 2019 report, the U.S. Senate Select Committee on Intelligence wrote that "all 50 states probably were scanned" by the GRU, but found no evidence "that any voter registration data was altered or deleted."

Another vector of attack could be an availability attack, which is when a hacker prevents a service from being available or responsive. In many states, poll workers access voter registration databases electronically to check in in-person voters (see the following section on poll books). An availability attack could prevent or slow this process, resulting in long wait times. Also, the U.S.'s largely voter-initiated registration system necessitates that states have public-facing websites which must maintain availability, even when traffic spikes. These websites are vulnerable to the threats faced by any website, including denial of service (DoS) attacks or misconfigured firewalls. The potential damage resulting from an availability attack on registration systems during the period where voters are eligible to register can be illustrated by two examples from 2020. While two situations—in Florida and Virginia—were not the result of malicious attacks, they underscore the problems that can result when a voter registration system goes down. They also make clear that not every state has yet implemented the safeguards necessary to keep these systems running or respond when they go down.

In Florida, on the last day for voter registration in 2020, pop star Ariana Grande tweeted out a note encouraging her followers to register, causing traffic to spike up to 1.1 million requests per hour. Probably due to a combination of high traffic and misconfigured servers, the voter registration system became unavailable for a critical time period, leading to chaos and litigation. A judge upbraided Florida's election officials, saying: "This court notes that every man who has stepped foot on the Moon launched from the Kennedy Space Center, in Florida… Yet, Florida has failed to figure out how to run an election properly—a task simpler than rocket science."

In Virginia, the online voter registration system also went down on the last day of availability in 2020, due to an accidentally cut fiber optic cable. This also led to litigation seeking an extension of the registration deadline. Unlike in Florida, the judge extended the registration deadline by 48 hours.

Because each state maintains a separate voter registration system, states can differ massively in their approaches to maintaining availability, security, and accuracy. As with all internet-connected systems,

attacks can be mitigated or prevented by following best cyber hygiene practices, such as using multi-factor authentication, strong passwords, secure cloud software services, encrypted data connections and frequent backups.

Poll books

In-person voting happens on Election Day, but some states also permit in-person voting before Election Day. Even with the rise in absentee and mail-in voting due to the COVID-19 pandemic, in-person voting is still used by a majority of voters (see the following section on absentee and mail-in voting).

At polling places—whether on Election Day or for early voting—voters must be checked in to ensure that they are registered, and that they have not already voted. Traditionally, election officials have used printed poll books, with entries for each voter eligible to vote at a given polling place. Assuming that the voter registration databases producing the poll book are secure, paper is a secure and reliable way to check in voters.

States increasingly, however, use internet-connected electronic poll books ("e-poll books") to check in voters. The number of in-person voters checked in with e-poll books more than doubled from 2012 to 2016, and then again increased by 48% from 2016 to 2018. Thirty-six states used e-poll books in 2018. E-poll books may take the form of software run on commercially available laptops or tablets, or dedicated commercial devices. Some states have developed their own e-poll book systems in-house.

E-poll books can be desirable for a few reasons:

- They may speed up the check-in process.
- They enable jurisdictions to streamline voting. Because they can be updated with the latest data, e-poll books enable jurisdictions to use a vote center model. Traditionally, polling places have been organized by precinct, with each precinct designated for a relatively small number of voters. In a vote center model, though, voters can check in at any polling place within a jurisdiction. Such a system requires e-poll books, so that a voter who has voted at one location can be marked digitally and made ineligible to vote again at a different location.
- Enable same-day changes. E-poll books enable poll workers to make real-time updates to the voter registration database, including registering voters in states that allow same-day registration.

At the same time, e-poll books also introduce vulnerabilities to an elections system. The benefits of e-poll books depend on their being connected to a network, which increases vulnerability to cyber attacks, especially if the network is the internet. For instance, the effects of an availability attack can be seen by several well-documented cases where issues with the e-poll books resulted in long delays:

- E-poll books took hours to sync their voting lists, causing delays in the 2020 primary election in Louisiana.
- Communication problems between e-poll books and the voter registration database halted voting in one county for four hours during the 2018 general election in Indiana.

- Problems with the wireless networks used for e-poll books slowed down voting in the 2020 primary election in Maryland.

- E-poll book issues caused long lines in the primary election, and in the first days of early voting in the general election, in 2020 in Georgia.

These issues, while not resulting directly from cyberattacks, underscore the importance of reliable e-poll book systems, and the damage that could be done by a successful attack that made e-poll books non-functional or unreliable. Having paper backups may mitigate problems; this year, a county in Ohio was able to switch to paper poll books after having difficulties with its e-poll book system early on Election Day.

One final issue is that, unlike with voting equipment, there are no federal regulations for e-poll books; the VVSG does not currently apply to them. But the EAC is partnering with a nonprofit to pilot a technology verification program focused on the security of non-voting election technology like e-poll books. This might reveal issues with e-poll book systems and offer a path forward for including them in the VVSG and certifying them.

Voting machines

The machines used in polling places for casting and recording votes have been a subject of great attention since the 2000 presidential election, which hinged on a razor-thin vote margin in Florida. The election highlighted a number of issues related to devices voters use to cast votes, one of which was the punchcard ballots used in Palm Beach County, Florida.

With punchcard ballots, voters indicate their choice by using a tool to punch out a square in a piece of paper. The square, or "chad," however, would not always be fully punched out, making it difficult to determine voter intent. HAVA created incentives and provided funding for municipalities, especially those using punchcard and other problematic systems, to upgrade to new equipment where voter intent could be made more clear.

The gold standard of ballot security and auditability is the hand-marked paper ballot, in which voters indicate their choice by using a pen or pencil to fill in a bubble next to their preferred candidate. The hand-marked paper ballot minimizes the number of electronic intermediaries involved in recording and tabulating the vote. Moreover, the hand-marking is a direct indicator of voter intent, enabling strong audits.

Electronic machines can also be used to cast votes, which provides some benefits but also poses new vulnerabilities. Electronic vote machines may be used by jurisdictions for a number of reasons. One important reason, for example, is to increase options for the disabled. About one in six eligible voters has a disability—such as blindness or another disability—that prevents them from physically marking a ballot without assistance. Electronic machines may enable the use of auditory and sip-and-puff interfaces, allowing voters with visual or motor disabilities, respectively, to cast their votes. HAVA requires that jurisdictions provide options for disabled voters to vote with the same privacy afforded to other voters. A jurisdiction may also want to use electronic machines for all voters to ensure that voters with disabilities are not using second-class equipment that is left to gather dust or unmaintained.

Like e-poll books, electronic machines may enable the voting center model, because they can display numerous ballot configurations applicable to each specific precinct in a given jurisdiction. A given county may have dozens of different ballot configurations, reflecting the different races (for, say, congressperson, school board member, or city councilperson) that a particular voter is eligible to participate in. Using electronic machines at voting centers is likely a better alternative than having hundreds or thousands of different printed ballots available at each center.

After HAVA was passed, many jurisdictions ended up purchasing direct-recording electronic (DRE) machines, which record the vote directly to memory on the same machine on which the vote was cast. DREs were perceived at the time to be cutting-edge technology, but in fact added severe new vulnerabilities to U.S. election infrastructure. In their 2019 report, the U.S. Senate Select Committee on Intelligence wrote:

> *While best practices dictate that electronic voting machines not be connected to the internet, some machines are internet-enabled. In addition, each machine has to be programmed before Election Day, a procedure often done either by connecting the machine to a local network to download software or by using removable media, such as a thumb drive. These functions are often carried out by local officials or contractors. If the computers responsible for writing and distributing the program are compromised, so too could all voting machines receiving a compromised update. Further, machines can be programmed to show one result to the voter while recording a different result in the tabulation. Without a paper backup, a 'recount' would use the same faulty software to re-tabulate the same results, because the primary records of the vote are stored in computer memory.*

Many DREs do not include a "voter-verified paper audit trail" (VVPAT), which means that, if something were to go wrong with the machine or the tally, it may be impossible to determine voter intent.

An improvement on DREs, especially those without a VVPAT, is the "ballot-marking device" (BMD) voting machine. With BMDs, voters select their choice and print out a ballot for review. As a separate step, that ballot is then scanned in a separate machine (see the following section on tabulation and reporting). Ballots frequently have a QR barcode encoding the choice, and a human-readable portion for verification and auditability. Although BMDs are preferable to DREs, some security researchers argue that they are still highly problematic. For example, a BMD may be hacked to record an incorrect vote on the ballot, either in the QR code or in the human-readable portion. A hacked QR code would be undetectable by the voter (though that would not affect an audit that used the human-readable portion). And it is possible that even an alteration of the human-readable portion would not be detected or reported, as voters rarely review BMD-printed ballots carefully.

Critical cyber vulnerabilities with many electronic voting infrastructure components, including DREs and BMDs, are similar. Many of them are based on commercially available hardware. On the one hand, this means that bugs may be found and patched quickly. But, unfortunately, many are running obsolete software that is no longer supported with security patches. And voting machines are "not as distant from the internet as it may seem," which means that it may be possible even for remote hackers to infect machines with malware. Moreover, machines may be deployed with default configurations, such as administrative or root-access passwords, giving an attacker easy access. Because of the severe impact of an availability or integrity attack, it is critical to insulate electronic election-related machines from the internet. It is also important to lock machines away physically and use tamper-evident seals to indicate whether the machine has been improperly accessed.

We turn now to a concept that, if adopted by election officials, could mitigate these concerns. In 2006, two leading security experts, Ronald L. Rivest and John P. Wack, defined the concept of "software independence," which applies to voting systems for which an undetected change or error in its software cannot cause an undetectable change or error in an election outcome. According to Rivest and Wack:

> *A voting system is software-independent if, after consideration of its software and hardware, it enables use of any election procedures needed to determine whether the election outcome is accurate without having to trust that the voting system software is correct. The election procedures could include those carried out by voters in the course of casting ballots, or in the case of optical scan and VVPAT, they could include election official procedures such as post-election audits.*

Fortunately, in the last 15 years or so there has been significant movement away from systems that do not include a VVPAT, and are therefore not software-independent. In 2016, 14 states had at least some jurisdictions using machines without VVPATs. By 2020, that number was brought down to just eight.

Software independence has been incorporated into the VVSG 2.0, which will likely increase its adoption. But while software independence is an important requirement for voting machines, it only ensures that election officials have the ability to determine that the outcome is correct. It does not ensure that every jurisdiction does in fact have processes in place to do that. Election officials must actually conduct audits to verify that an election has produced the correct outcome.

Absentee and mail-in voting

Since the Civil War, voters in the U.S. have been able to cast votes by mail. In general, there is no meaningful distinction between the terms "absentee" and "mail-in"—some jurisdictions use one term in their statutes and regulations, and some use the other.

Before 2020, absentee voting was available in every jurisdiction; but in many cases, a voter needed to have an excuse, such as being elderly or sick. But, in response to the global COVID-19 pandemic, many states made it easier to vote absentee, as a safety measure. Accordingly, about 40% of voters voted by mail in 2020, almost double the proportion from 2016.

As is likely to happen with any rapid change in election administration, 2020 saw some growing pains. The most common problem was administrator or vendor error that resulted in incorrect ballots sent to voters. This happened to some voters in Ohio, New Jersey, Pennsylvania, and New York City, among other places.

But the most serious issues related to absentee voting in 2020 relate to long-running and ongoing attempts to convince the public that mail-in voting was insecure and rife with fraud. This may have polarized the absentee vote, by convincing some voters that mailed ballots would not be properly counted. Perhaps as a result, Democrats were likelier than Republicans to request mail-in ballots. It's important to note that, despite this misinformation campaign, many of the same security checks for in-person voting also apply to absentee voting:

- Voter registration databases are used to ensure that only registered voters may cast a ballot, and that voters can only vote once (see the previous section on voter registration). Unique barcodes are used to tie each ballot to a specific registered voter.

- Voters attest, under penalty of perjury, that they are who they say they are.

- Voters sign their ballot envelopes. Those signatures may be compared to the signature on file to verify the voter's identity.

Furthermore, there are security benefits to mail-in voting. By spreading out voting infrastructure over time and space, mail-in voting decreases the number of high-value targets for would-be attackers. Whereas an attacker could cause a lot of damage by targeting in-person voting infrastructure at a time and place where many voters are expected to be (say, a populous precinct on Election Day), there are fewer obvious targets for mail-in voting.

Thanks to these security measures, and because there are severe penalties for voter fraud, absentee fraud is extremely rare—there is only about one case per state every six or seven years. Most importantly, there is no evidence of widespread voter fraud by absentee having ever occurred, including in 2020.

However, as with every technology or process, it is important to understand and mitigate novel or elevated vulnerabilities. For instance, higher levels of absentee voting increase the importance of ensuring that voter registration databases are secure from integrity attacks, as discussed above. Because voter registration databases contain the addresses to which blank ballots are sent, if an attacker alters the addresses, ballots could be sent to the wrong location. It could take time for voters and administrators to detect and rectify incorrect details, putting a voter at risk of missing the deadline for casting their ballot by mail.

Another possible vulnerability with mail-in ballots lies in their use of signature matching—a security measure used by many states—to verify that the ballot has been cast by the registered voter. When election officials in these states receive ballots, they compare the signature on an outer envelope to the signature in a voter registration database. If an attacker were to conduct a confidentiality attack in which they gained signatures, such as through an attack on the voter registration database or even on a separate system with signature images, they could perhaps forge signatures on mail-in ballots. (Security issues aside, it is worth noting that signature matching processes themselves may disenfranchise voters, especially those already marginalized; it is therefore important to notify voters when their signatures are deemed deficient, giving them an opportunity to fix their ballot.)

There is no evidence that either of the above hypothetical attacks has ever occurred, and certainly there has not been such an attack at scale. As with many attacks on election infrastructure, they would be difficult to scale without detection, and would expose the attacker to severe penalties.

Tabulation and reporting

Once physical ballots are cast, whether by mail or in-person, whether marked by hand or by a BMD, they must be scanned, tabulated, and reported. And ballot scanners, like many other electronic components, are just another type of computer that must be protected against infection by malware.

Scanning is either done centrally or at the precinct level, in each polling place. When scanning is done centrally, cast ballots are transported from precincts to a central location, to be processed by a high speed ballot scanner. One benefit of central scanning is that it requires less equipment, whereas scanning at precincts requires that each precinct have one or more scanners.

When scanning is done at the precinct level, voters insert their ballot directly into the scanner. A benefit of precinct-level scanning is that a scanner can immediately notify the voter if there is a problem, such as if the voter mistakenly selected multiple candidates in a race (also called an overvote), or if they missed a race (an undervote). The voter then has a chance to correct their mistake.

Again, there are important security considerations. Researchers have shown that certain models of optical scanners execute software on memory cards that could be replaced by an attacker, which could lead a scanner to produce an incorrect count. Although vulnerabilities with these models have been known since at least 2005, it appears that the vulnerable machines are still used by some precincts in 12 states.

For these reasons, whether using central or precinct scanners, it is critical to physically secure these machines by, for instance, blocking USB ports and locking them with tamper-evident seals.

Election officials must also secure any transmission lines used for communicating the count between election officials. Depending on the method of counting, and the types of ballots counted, this can include communication lines from precincts to counties, from counties to the state, and possibly others. If communication is disrupted by an attack, that could result in a delayed tally, or a temporarily incorrect tally (which would eventually be caught and corrected by various checks later in the process).

Officials should also secure public websites used to display results. If an attacker brought down, defaced, or modified a public results website, chaos and confusion might ensue—a possibility that concerned election officials in the 2020 election cycle. There do not appear, however, to have been any successful attacks on reporting systems in 2020.

However, other issues in the 2020 election year can serve to illustrate the disastrous effect of a delay in reporting. Because election officials in key states were not allowed to count and report absentee ballots until late in the process, some results were slow to arrive, leading to apparent (but misleading) shifts in which candidate was leading. This uncertainty, which was not explained particularly well by much of the media, set the stage for conspiracy theories to spread, and for election officials to be targeted with death threats. An attack that produced a similar delay in reporting in key states, or that produced an error that needed to be reversed, would create similar opportunities for dangerous misinformation to proliferate.

Individuals involved in elections

Perhaps the cyber attack with the greatest impact on an American election did not target a voting system, but a campaign: the Russian attack on the personal email account of John Podesta, campaign chairman for Hillary Clinton's 2016 presidential campaign. Russian cyber attackers sent an email to Podesta, urging him to reset his email password. After receiving advice that was incorrect (possibly due to a typo) about the legitimacy of the email, Podesta provided his password to the attackers. The attackers were then able to access his email account, and slowly published his emails in a way that dominated media coverage leading up to the election.

This type of attack, called a spear-phishing attack, is when a deceptive email is sent to a specific individual or organization, intended to obtain the user's login credentials. A 2019 Symantec analysis said that spear-phishing was the most popular avenue of attack for known hacker groups.

Another high profile spear-phishing incident from 2016 targeted an elections vendor. The 2019 Special Counsel report shows that the GRU successfully spear-phished employees of an election vendor, gaining access to a network internal to a Florida county:

> *[GRU] Unit 74455 also sent spear phishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of [REDACTED], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spear-phishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election. The spear-phishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer. The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government.*

These examples illustrate that individuals doing work related to an election, whether for a campaign, an election office, or a private vendor, may be vulnerable to phishing and other schemes intended to obtain access credentials. Obtaining credentials can enable an attacker to carry out any number of attacks. In addition to a confidentiality attack of the kind that targeted Podesta, an attacker could also carry out an availability attack, potentially disrupting the mechanics of the election itself, or an integrity attack, targeting voter rolls or election results.

Post-election audits

The best practices listed below are intended to improve the security of the above components of election infrastructure. But because it is impossible to completely guarantee the security of any system, post-election audits serve as a critical safeguard for detecting some problems that may have occurred.

There are many forms of post-election audits. Election officials may check to ensure that proper procedures were followed during the election. An audit of this type may involve verifying, for instance, that the number of ballots voted at a precinct matches the number of people checked in at the poll books. Or it may involve spot-checking tabulation equipment to see if they are operating properly.

Traditional tabulation audits

Perhaps the most important kind of audit looks at the VVPAT to ensure that the outcome is correct. Tabulation audits use direct evidence of voter intent (as recorded by the VVPAT) in an attempt to verify that the outcome of an election is correct, which can mitigate vulnerabilities in the chain between ballot casting and ballot tabulation. Traditional audits, which are required by law in most states, select a random sample of ballots (say, all the ballots in 3 percent of precincts) to be counted by hand; if those results differ substantially from the machine tally, a full hand recount is triggered.

But these traditional audits are not able to provide any quantifiable degree of confidence in the election. Moreover, they can be both inefficient and under-informative. In an election with very wide margins, a traditional audit might count far more ballots than is necessary to have confidence in the outcome. And in a very close election, counting every ballot in 3 percent of precincts may not be enough to know whether the election's outcome was correct. Fortunately, there is a better option that addresses these issues.

Risk-limiting audits

The risk-limiting audit (RLA) is a relatively new technique that can efficiently produce a high degree of statistical confidence that the election outcome was correct, sometimes after sampling only a very small number of ballots.

In an RLA, administrators repeatedly select random samples of ballots, until they reach a pre-specified degree of confidence that a full hand recount would not change the winner. When the margin separating the leading candidates is wide, a RLA may only require a small number of ballots to be sampled to gain confidence. But if the margin is close, the RLA may require many more ballots. This efficiency means that it should be possible to conduct RLAs for all federal elections at relatively low cost—perhaps about $20 million a year.

Six states now have statutory requirements for an RLA or an RLA pilot. The continued adoption of RLAs can efficiently build trust and confidence in electoral systems and outcomes.

Best practices and policy considerations

For election officials

The following is a consolidated list of mitigation options that state and local election officials may consider and may have the authority to implement immediately. For election officials seeking more detail, CDT has worked with the Center for Tech and Civic Life to develop a course on cybersecurity for election officials.

- Ensuring that all software is patched and up-to-date.
- Using multi-factor authentication wherever possible.
- Using strong passwords and password managers.
- Implementing services that mitigate DoS and DDoS attacks.
- Using secure cloud software services to improve reliability and security.
- Regularly backing up critical data, like voter registration databases.
- Monitoring of voter registration databases to detect intrusions.
- Physically securing all machines, including e-poll books, voting machines, and ballot scanners. Storage in secure facilities, use of port blockers, and use of tamper-evident seals.
- If using e-poll books, ensuring availability of paper backups.
- Ensuring polling place internet connections are reliable and secure.
- Maximizing the use of voting methods with VVPATs.
- Replacing outdated paperless DRE systems with auditable, software-independent systems.
- Where BMDs are used, maximizing the likelihood of voters actually checking the printed ballot before it is scanned, through good ballot design, instructions, and signage.
- Where permitted under state law, permanently expanding eligibility for absentee voting, reducing the risk of attack on election infrastructure by spreading out voting over time and space.

- Protecting individuals from phishing attacks, including by training users to spot phishing emails, and implementing phishing email filters.
- Participating in cyber security assistance programs offered by federal agencies like CISA and EAC, such as vulnerability scanning and remote penetration testing.
- Facilitating adversarial testing of computerized election-related systems.
- Piloting and implementing risk-limiting audits for all federal elections.

For Congress and federal agencies

Although election officials can do a lot to secure election infrastructure, there are many options available for federal lawmakers and agencies to improve security and give election officials important resources.

- Raising federal minimum standards for elections, such as by mandating or incentivizing the use of paper-based systems.
- Incentivizing jurisdictions to pilot and implement risk-limiting audits.
- Providing increased, regular funding to allow states to implement best practices and upgrade voting equipment where needed.
- Increasing funding for the EAC, which is well-equipped to help jurisdictions improve their election systems.
- Creating an industry-wide coordinated vulnerability disclosure program, facilitating independent security research, and the coordination of rapid responses to vulnerabilities discovered by researchers.
- Continuing to improve communication and coordination between election officials and security officials at all levels (federal, state, local, tribal, and territorial).
- Increasing staffing levels at CISA, to support its mission of bolstering election security.
- Continuing to develop and update CISA's catalog of cyber security assistance programs.
- Considering the addition of non-voting election technology, such as e-poll books, to the definition of "voting system" for inclusion in the voluntary voting systems guidelines.
- Promoting the passage of the "Securing America's Federal Elections Act" (SAFE) Act, which may help accomplish many of the above listed improvements.
- Expanding and promoting voter education programs, such as CISA's rumor control page about how elections work, why they are trustworthy, and what election officials do.

Conclusion: Strong cybersecurity is fundamental to trust in elections

As we have illustrated, the election cybersecurity landscape is diverse and complex. The patchwork system in the U.S. will always pose significant challenges to the security of its national elections. Between 2016 and 2020, the U.S. made major strides improving election security: election officials upgraded and tested their systems, federal agencies improved threat communication and response, and officials bolstered protection against phishing threats. But there are persistent issues with software and hardware that can never be fully solved, which means that while it is important to improve the software and hardware, it is equally important to implement rigorous and vigilant processes to train officials, improve coordination, and audit results.

The 2020 general election highlighted that attacks and, especially, malign information operations have evolved since 2016. Voter suppression content operations flourished, in which voters are confronted with information that could discourage or prevent them from casting their ballot. In 2020, these operations have included misinformation about how votes are cast, and how elections are kept secure.

In the face of these threats, it is important to build public trust. Many of the above improvements accomplish two goals: First, they materially increase security. Second, and just as important, they increase trust, which is foundational for a functioning democracy. Certainly, conspiracy theories and misinformation about election integrity, fraud, or rigging, can circulate even in the absence of any concrete evidence. But one way to reduce the spread of misinformation is to run elections in a secure and efficient way that is inherently trustworthy.

The U.S. is making steady improvements as evidenced by the increased use of voting machines with VVPAT, the increased adoption of RLAs, and the rapid expansion of absentee voting. But threats are always evolving. In order to remain steps ahead of attackers, the U.S. is well advised to continue upgrading and improving equipment and processes, recognizing that good security is a process, not an endpoint.

Authors

William T. Adler

Senior Technologist, Elections & Democracy

CENTER FOR DEMOCRACY & TECHNOLOGY

William is the Senior Technologist in Elections & Democracy at CDT, where he works to ensure that American elections are fair, accessible, and secure.

Before joining CDT, William worked on tech issues in the office of U.S. Senator Elizabeth Warren. He also worked at the Princeton Gerrymandering Project at Princeton University, advancing the causes of redistricting reform and open election data. He has published pieces in numerous peer-reviewed journals and popular press outlets, including the New York Times, FiveThirtyEight, and Scientific American.

William holds a BA in Psychology from Carleton College and a PhD in Neuroscience from New York University. His website can be found here.

Mallory Knodel

Chief Technology Officer

CENTER FOR DEMOCRACY & TECHNOLOGY

Mallory Knodel is CDT's Chief Technology Officer. She is the co-chair of the Human Rights and Protocol Considerations research group of the Internet Research Task Force and an advisor to the Freedom Online Coalition. Mallory takes a human rights, people-centered approach to technology implementation and cybersecurity policy advocacy.

Originally from the US, having lived extensively in Nairobi before coming back to DC, she has worked with grassroots organizations around the world in Bolivia, France, Palestine and the UK. She has used free software throughout her professional career and considers herself a public interest technologist. She holds a BS in Physics and Mathematics and an MA in Science Education.

The Konrad-Adenauer-Stiftung (KAS) is a German political foundation and think tank. Worldwide, KAS is in charge of over 200 projects in more than 120 countries, where it promotes freedom and liberty, peace, and justice. KAS also focuses on consolidating democracy, the unification of Europe and the strengthening of transatlantic relations, as well as on development cooperation. The KAS office in Washington DC was established in the late 1970s and to this day it stands for and sees itself as a promoter of these values.

Published by:

Konrad-Adenauer-Stiftung USA
2005 Massachusetts Avenue, NW
Washington, D.C. 20036
U.S.A.
Tel.: +1(202) 464-5840
www.kas.de/usa

KONRAD
ADENAUER
STIFTUNG

Konrad-Adenauer-Stiftung USA
2005 Massachusetts Avenue NW
Washington, DC 20036
U.S.A.
www.kas.de/usa