

Appendix

A: City of Conyers Pilot Project Report (referenced on pages 14 and 15)

B-D: Documents Submitted by Commission Member Dr. Wenke Lee (referenced on pages 15 and 16)

1. Cybersecurity Considerations for Voting Systems
2. Basic Security Requirements for Voting Systems
3. Addendum to Basic Security Requirements for Voting Systems

E: Comments Submitted by Commission Member Lynn Bailey

F: SAFE Commission Dissenting Report Submitted by Commission Members Senator Lester Jackson, Representative James Beverly, and Mike Jablonski

City of Conyers Pilot Project Report

Georgia Secretary of State's Office

FEBRUARY 1, 2018

City of Conyers Pilot Project Report

Executive Summary

The Georgia Secretary of State's Office, in partnership with the City of Conyers and the Rockdale County Board of Elections and Voter Registration, conducted a pilot project to test new voting equipment with a voter-verifiable paper ballot during the November 7, 2017, municipal elections in Conyers. The piloted equipment was used for both advance voting and on Election Day.

The Secretary of State's Office tested a system that utilized ballot marking devices and precinct-based optical scanners. There were no fees or costs incurred by the Secretary of State's Office, the City of Conyers, or the Rockdale County Board of Elections and Voter Registration to use the equipment for this test.

The voting system used for this pilot project was the Elections Systems and Software (ES&S) EVS 5.2.2.0 comprised of ExpressVote Universal Voting Systems (ExpressVotes) and DS200 precinct-based scanner and tabulators (DS200s). ExpressVotes are touch-screen ballot marking devices that voters use to indicate and print their selections on paper ballots. The DS200 precinct-based scanner and tabulators are optical scanners that identify, record, and tally voters' selections and save them to a military grade encrypted USB memory drive used for final tabulation. The DS200 units also have ballot boxes that securely retain voted and scanned paper ballots. Additionally, the DS200s save a digital image (front and back) of each ballot cast. The number of units used for the pilot project was based on a 1:1 ratio of ExpressVotes to the number of Direct Recording Electronic (DRE) voting machines the county would normally deploy and two DS200s per polling place.

The Rockdale County Board of Elections and Voter Registration reported no issues during advance voting or on Election Day. The unofficial results were fully reported at 8:10 PM on Election Day.

To assess voter confidence and satisfaction with the piloted equipment, the Secretary of State's staff conducted an exit poll during each day of advance voting and on Election Day. With over 65% of all voters participating in the survey, the results were overwhelmingly positive.

1. On a scale of 1 to 10 with 10 being the most satisfied using the piloted equipment, the average response was 9.21.
2. On a scale of 1 to 10 with 10 being very confident that their vote was counted accurately, the average response was 9.28.
3. 65.99% of voters surveyed indicated that they preferred voting on the piloted system.

As evidenced by the exit polling, the piloted system had high levels of voter confidence and satisfaction. This combination of ballot marking devices and precinct-based scanner and tabulators provides voters with a similar voting experience to the currently used DREs (making selections on a touch-screen), but also addresses the desire for a voter-verified paper ballot.

Based on the feedback received from Rockdale County election officials, this type of system also appears to improve the county's administrative experience. As seen during this pilot, this type of system saves counties time during their opening and closing procedures, allows them to report results faster, and maintains critical functionalities that the counties are accustomed to with the state's current system.

City of Conyers Pilot Project Report

Background

The Georgia Secretary of State's Office, in partnership with the City of Conyers and the Rockdale County Board of Elections and Voter Registration, conducted a pilot project to test new voting equipment with a voter-verifiable paper ballot during the November 7, 2017, municipal elections in Conyers. The piloted equipment was used for both advance voting and on Election Day.

The decision to pilot new equipment in 2017 was threefold. First, while the Secretary of State's Office is confident in the security and operation of the state's current voting system, it is prudent to research other available systems given the age of the current system. Second, the Secretary of State's Office believes that viable, vetted replacement options now exist based on the technology, security, and design of the voting systems currently available on the market. Finally, since Georgia law does not require municipalities to use Direct Recording Electronic (DRE) voting machines as required in other elections, the 2017 municipal elections presented an opportunity to begin testing different equipment without violating state statute.

The Secretary of State's Office selected Conyers to host the pilot project because of the City and the Rockdale County Election Board's willingness to participate, the expertise and experience of the Rockdale County elections staff contracted to administer the City's elections, and there were no state-level special elections that overlapped the city's jurisdiction. Conyers' close proximity to the Secretary of State's Office in Atlanta also allowed state staff to conduct daily exit polling.

Additionally, the Secretary of State's Office chose to test a system offered by Elections Systems and Software (ES&S) due to its functionality, auditability, and the vendor's ability to interface with the state's current ballot building and electronic pollbook software that is proprietary to ES&S. There were no fees or costs incurred by the Secretary of State's Office, the City of Conyers, or the Rockdale County Board of Elections and Voter Registration for use of the vendor's equipment for this test.

Both the Rockdale County Board of Elections and Registration and the Secretary of State's Office worked to educate voters, the media, and legislators about the pilot program and equipment being tested. On September 5, 2017, Rockdale County hosted members of the media at its office to demonstrate the system and answer questions. Similarly, the Secretary of State's Office invited all members of the Georgia General Assembly to a system demonstration held on October 5, 2017, in the state Capitol.

Equipment and Election Operations

The voting system used for this pilot project was the ES&S EVS 5.2.2.0 comprised of ExpressVote Universal Voting Systems (ExpressVotes) and DS200 precinct-based scanner and tabulators (DS200s). ExpressVotes are touch-screen ballot marking devices that voters use to indicate and print their selections on paper ballots. All ExpressVote units are equipped with ADA-compliant keypads and headsets for disabled voters. The DS200 precinct-based scanner and tabulators are optical scanners that identify, record, and tally voters' selections and save them to a military grade encrypted USB memory drive that is used for final tabulation. The DS200 units also have ballot boxes that securely retain voted and scanned paper ballots. Additionally, the DS200s save a digital image (front and back) of each ballot cast.

This system was certified by the Election Assistance Commission (EAC) on February 27, 2017, passed state testing on September 5, 2017, and was provisionally certified by the Secretary of State's Office on

City of Conyers Pilot Project Report

September 18, 2017. Acceptance testing was completed on the piloted equipment on September 20, 2017, and the Rockdale County Board of Elections and Registration conducted public logic and accuracy testing on October 2, 2017, as is required before every election.

Allocation

The following number of units were used for the pilot project based on a 1:1 ratio of ExpressVotes to the number of DREs the county would normally deploy and two DS200s per location:

- Advance Voting: October 16, 2017 to November 3, 2017
 - 7 ExpressVotes (ballot marking devices)
 - 2 DS200s (scanner/tabulators)
- 001 Conyers Precinct- Election Day Polling Location: November 7, 2017
 - 4 ExpressVotes (ballot marking devices)
 - 2 DS200s (scanner/tabulators)
- 002 Olde Towne Precinct- Election Day Polling Location: November 7, 2017
 - 6 ExpressVotes (ballot marking devices)
 - 2 DS200s (scanner/tabulators)
- Absentee and Provisional- Rockdale County Elections Office
 - 1 DS200 (scanner/tabulator)

Additional ExpressVotes and DS200s were on hand at the Rockdale County Elections Office if there was an issue with a unit in use. No backup devices were deployed.

The equipment ratio indicated in this report does not reflect a required ratio, but rather the quantities used for evaluation as part of this pilot.

Voter Experience

The check-in and voting process went as follows during advance voting and on Election Day:

- Voters checked in as usual, with poll workers using laptops during advance voting and the state's current electronic poll books (ES&S ExpressPoll 5000s) on Election Day. After checking-in voters, poll workers used ExpressVote printers to print the voters' card with their ballot style. (This ballot style tells the ballot marking device which ballot to pull up to match the voters' specific districts. No personal identifying information is on the ballot.)
- Next, voters were given a card to feed into an ExpressVote ballot marking device. The voters then selected their choices on the touch-screen. Those choices were thermally printed onto their paper ballot once they reviewed their choices and selected "Print Card."
- Once voters selected "Print Card," the ballot was printed and voters reviewed their choices again. If there was an issue with their ballot or they wanted to change their vote, they could have alerted a poll worker and started the process again.
- After reviewing their choices on the paper ballot, the voters then fed their ballot into a DS200 precinct-based scanner and tabulator. After digitally scanning and recording the votes indicated on the ballot, the machine secured the paper ballot in a locked box.

Tabulation

All vote totals and ballot images were stored on military grade encrypted USB memory drives and secured within the DS200s. After the polls closed, the encrypted drives were collected and uploaded to a central election management system (ElectionWare version 4.7.1.1) to conduct a final tabulation of the

City of Conyers Pilot Project Report

results. If a candidate had requested a recount following the election, the voted paper ballots would have been available in addition to scanned ballot images and the counts on the encrypted drives; however, no recount was requested.

The Rockdale County Board of Elections and Voter Registration reported no issues with closing and tabulating procedures. The unofficial results were fully reported at 8:10 PM on Election Day.

County Perspective

While the Secretary of State's Office initiated and coordinated the pilot project, it would not have been possible without the hard work of the Rockdale County Board of Elections and Voter Registration. The Rockdale County elections team, led by Elections Supervisor Cynthia Welch, worked tirelessly to ensure that its poll workers and voters were prepared to use this new equipment in a real-life test.

While the Rockdale County Board of Elections and Voter Registration plans to release its own report detailing its experience with the pilot program, the Secretary of State's Office wanted to highlight the county's perspective and insight in this report. Cynthia Welch stated the following:

I wanted to express how satisfied the voters, election workers, staff, and I were with the pilot project experience.

Rockdale County was the only jurisdiction selected to conduct a pilot during the 2017 municipal elections, and we gladly accepted. We began working with the piloted system in September to conduct logic and accuracy testing, and compared to testing the DREs, this was a much simpler task. Early voting began on October 16, 2017, and concluded on November 3, 2017. Our early voting election workers opened and closed the precinct each day in record time (less than 5 minutes to close).

Additionally, Election Day poll worker training was a breeze and workers adapted quickly to the new system. The overall response from our poll workers was that the setup, opening, and closing procedures were much easier than what is currently required with the DREs.

On Election Day, the Rockdale County elections staff closed out the early voting DS200 tabulators and fed the mail-in absentee ballots through the DS200 tabulator with ease. At 7:00 PM, we uploaded our first results, providing them to the public in record time. By 8:10 PM, all unofficial results were reported without any problems.

I am happy to report that we received an overwhelmingly positive response from our voters, and they required very little assistance using the ExpressVotes, including inserting ballots into the DS200 tabulator. Overall, voters seemed quite happy to see a system that would give them a verifiable paper ballot which they could review before casting.

We enjoyed conducting this pilot and hope that our feedback will help to create a greater experience for jurisdictions and voters across the state.

City of Conyers Pilot Project Report

Exit Poll

In order to assess voter confidence and satisfaction with the piloted equipment, the Secretary of State's staff conducted an exit poll during each day of advance voting and on Election Day. As voters exited a polling location, they were asked if they would like to take a brief survey on their voting experience.

Survey Questions

Participants were asked the following three questions and given an opportunity to comment:

1. How satisfied were you with using the voting equipment?
 - Answer options were: 1-10 with 1 being "Not Satisfied at All" and 10 being "Very Satisfied"
2. Based on your experience with the voting equipment today, how confident are you that your vote was counted accurately?
 - Answer options were: 1-10 with 1 being "Not Confident at All" and 10 being "Very Confident"
3. Today we are testing out new voting equipment that combines an electronic ballot marking device with a paper ballot to improve the voting experience. If you have voted in the past on an electronic voting machine, would you prefer to use an electronic voting machine or the equipment you used today to vote?
 - Answer options were:
 - i. "I have not voted before on an electronic voting machine."
 - ii. "Electronic ballot marking device with a paper ballot (what was used today)."
 - iii. "Electronic voting machine (DRE)."
 - iv. "No preference."
 - v. "Other." (Participants could add comments).
4. General Comments and Suggestions:
 - Answer optional.

Results

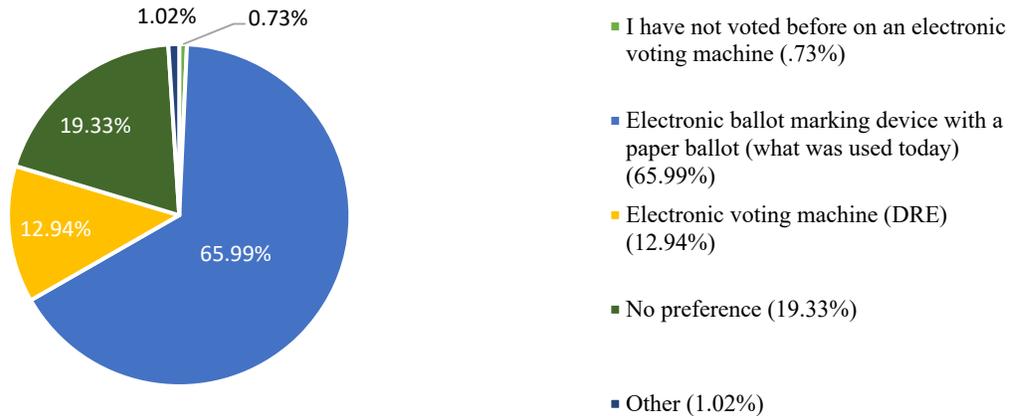
Of the 1,054 people who voted in the November 7, 2017, City of Conyers elections, 688 (65.28%) participated in the exit poll.

The results were:

1. On a scale of 1 to 10 with 10 being the most satisfied using the equipment, the mean response of the 686 participants that answered this question was 9.21.
2. On a scale of 1 to 10 with 10 being very confident that their vote was counted accurately, the mean response of the 684 participants that answered this question was 9.28.
3. Of the 688 voters that answered this question, the results on equipment preference were:

City of Conyers Pilot Project Report

Question 3: Equipment Preference



4. Question 4: 84 (12.21%) participants provided comments and suggestions. Individual voter responses will be provided upon request.

**Please see Attachment A for additional data analysis provided by the University of Georgia School of Public and International Affairs.*

Conclusion

As evidenced by the exit polling, the piloted system had high levels of voter confidence and satisfaction. This combination of ballot marking devices and precinct-based scanner and tabulators provides voters with a similar voting experience to the currently used DREs (making sections on a touch-screen), but also addresses the desire for a voter-verified paper ballot.

Based on the feedback received from Rockdale County election officials, the use of this type of system appears to improve the county's administrative experience as well. As seen during this pilot, this type of system saved counties time during their opening and closing procedures, allowed faster reporting of results, and maintained functionalities, like being able to quickly provide all ballot styles needed during advance voting.

While this pilot project was a successful first test of new equipment, the Secretary of State's Office would like to conduct additional testing in the future to assess other potentially viable voting system replacement solutions.

Cybersecurity Considerations for Voting Systems

Wenke Lee, Ph.D.
wenke.lee@gmail.com

This document provides a very brief overview of cybersecurity and discusses the design considerations for secure voting.

As presented to the Georgia Office of the Secretary of State's "Secure, Accessible & Fair Elections (SAFE) Commission," on Aug. 30, 2018.

Wenke Lee

- **Work at Georgia Tech (2001-)**
 - Professor of Computer Science, John P. Imlay Jr. Chair
 - Co-Executive-Director of the Institute for Information Security & Privacy (IISP)
 - Teach cybersecurity to 2,500 students/year
- **Researcher in cybersecurity (1994-)**
 - Ph.D. in 1999 from Columbia University (Thesis: a machine learning framework for intrusion detection)
 - Systems and network security, malware analysis, botnet detection, cryptography; Damballa (Core Security)

My name is Wenke Lee and I am a professor and John P. Imlay Jr. Chair in the School of Computer Science, College of Computing, at the Georgia Institute of Technology.

I am also a co-executive director of the Institute for Information Security & Privacy (IISP) at Georgia Tech -- the coordinating body for 13 cybersecurity research labs at Georgia Tech which together performed more than \$144 million in research for government, defense, and corporate partners last year (FY2018, ended June 30, 2018). The IISP's mission is to unify research scientists, faculty and students across multiple fields -- such as Engineering, Business, and Public Policy -- to support comprehensive research, new educational pathways, and the tech-transfer that moves our discoveries out of the university and into the marketplace.

I have been a researcher in cybersecurity for more than 20 years. I received my Ph.D. in Computer Science from Columbia University in 1999. For my thesis research, I developed a machine learning framework for intrusion detection.

I have been a professor since 1999. Today, I teach several cybersecurity classes at Georgia Tech to approximately 2,500 on-campus and online degree students per year.

I also continue to perform cybersecurity research for partners such as DARPA, the Office of Naval Research Labs, National Science Foundation, Intel and others. I have published over 100 peer-reviewed papers in top academic venues about systems, network, and software security; malware analysis; botnet detection; authentication, and data encryption. Some of my research about botnet detection was used to start an Atlanta-based company, called Damballa, which was later acquired by Core Security.

SAFE Commission

- Work and opinion: my own
- Input from researchers in voting system security

The security and integrity of our voting system is essential for our democracy, and so I am truly honored to serve on the SAFE Commission. I have been a citizen of the United States for nearly 20 years. I deeply appreciate that within a democracy, you can advocate for yourself and for others, that you can shine light on policies that need improvement, and openly discuss better approaches to self government. The choices we make on election day are central to this process and the election process must be protected in every way .

My work for the SAFE Commission is my own and therefore my opinions do not necessarily reflect those of Georgia Tech.

I rely on my decades of experience in cybersecurity, as well as input from computer science and engineering researchers working in the area of voting system security. I have been reading their papers and reports, and I have had direct discussions with them about various voting security issues.

Vulnerabilities In Voting Systems

- There will always be ... not news!
- Vulnerabilities = errors/weaknesses that can be exploited by attackers
- No system can be shown to contain no error
 - Developed by engineers/programmers
 - Chrome: 7 million lines of code, Android: 15 million
Windows: 50 million, Car: 100 million+
 - *Can you write/edit a book that thick without an error?*

We often hear in the news that a cyberattack or a hack occurred, and unfortunately, lately some of those news stories involve voting systems. Typically, a cyberattack occurred because an attacker was able to exploit a vulnerability in a cyber system.

I am never surprised when I hear news about any cyberattack. There is an established theorem that states, “there is no way to know for sure that any real, useful system contains no vulnerability.” That is, even if we carefully engineer and test a system, we still cannot be sure that it has no vulnerability (or no error); and much more likely than not, any system will have some security vulnerabilities.

This should not be a surprise given how complex today’s systems are: for example, Chrome has 7 million line of code, Android has 15 million, and Windows has 50 million, and a typical automobile control system has 100 million lines of code. Cyber systems are developed and tested by programmers and engineers, and so errors introduced by humans are not avoidable.

EVERY System Is At Risk

- Not if but when, how much can we find out?
- Even sophisticated, high-profile organizations have been attacked
 - e.g., OPM, HomeDepot, Equifax
- Many organizations seek public help to secure their systems
 - DoD, Google, Apple, Tesla, United Airlines

We often say that the question is not IF an organization will be hacked; it is WHEN, and how much can we find out about the damage afterward. This is because every system is likely to have security vulnerabilities.

Even high-profile organizations, such as HomeDepot and Equifax, can be vulnerable despite investing a lot of resources in security protection. Organizations continually must go to great lengths to improve their security protection.

It is commonplace now for companies to offer “bug bounties” -- financial rewards to anyone who openly hacks, finds, and discloses security vulnerabilities in their products, services, and operations. Tech giants, airlines, even the U.S. Marine Corps have publicly advertised and invited hackers to comb their systems for flaws **and report them**.

These types of hacks are invited by the organization, seen as helpful to the organization, and performed by “white-hat hackers” who are acting for the public good. Within cybersecurity circles, we always say it is better that a White Hat or academic researcher find your flaws, because we report them when we do. The bad guys don’t.

The reporting of flaws can be made directly to the organization, to a vendor responsible for the flaw, and/or to a federal organization such as the U.S. Department of Homeland Security CERT team – the Computer Emergency Readiness Team.

The point here is that everyone is vulnerable, everything is at risk, and it takes a community to help counter cyberthreats.

Cybersecurity Is VERY Hard



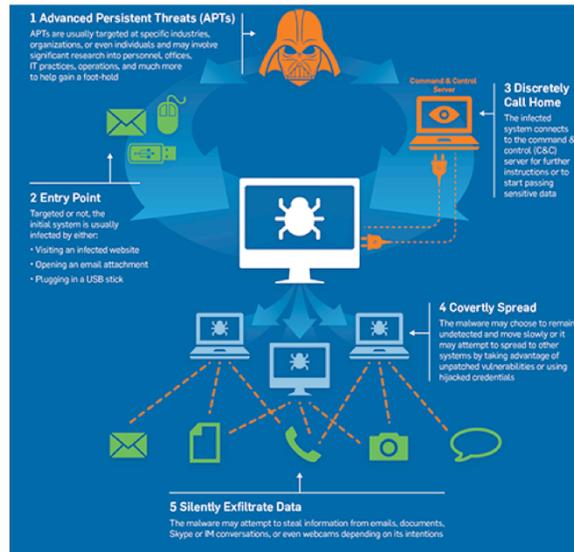
Why can't we just secure our cyber systems?

First, in order to do so, we need to know what vulnerabilities our systems have and fix them all. But if that is achievable, it would mean we have found a way to show that a (fixed) system has no vulnerability, which is a contrary to the established theorem. In short, **we can never know that we have completely secured any system.**

Second, attacking is inherently easier than defending because it needs to only find and exploit the weakest link in a system or organization. And attack technologies have advanced significantly since the late 1990s to become easily accessible to any would-be attacker. For example, an attacker can “buy” and deploy malware that exploits a previously untapped vulnerability to compromise a large number of computers or just target a specific organization.

Or he can simply “rent” the right to use a list of already compromised computers, known as “bots” which have a vulnerability that has not been patched. Simply put, attacks have become easier and hence more prevalent.

Advanced Persistent Threats



A particularly dangerous kind of attack is the so-called “Advanced Persistent Threat” (APT). Such an attack aims to quietly carry out its malicious activities so that it is hard to not only detect the attack but also access the damage upon detection.

An APT attack starts by compromising a computer (or a user account) via many means, including phishing emails, compromised web sites, “free” USB thumb drives, etc. Once it succeeds in injecting a malware to run on a compromised computer, the malware connects to the attacker’s computer to receive commands and updates, and accordingly carry out the intended attack, such as spreading the malware to other vulnerable computers or user accounts in the organization and exfiltrating any valuable data to the attacker’s computer. APT malware is designed to carry out activities below the detection threshold, e.g., transmitting data in small volume or only when the user is also browsing the web, and even removing all evidences to cover its tracks as it moves from one computer to the next.

Achieving Cybersecurity

- Secure = not vulnerable to cyber attacks
- Option #1: Don't use any cyber component
 - Because we can't guarantee zero vulnerabilities
- Option #2: Keep away would-be attackers
 - But the cyber world is VERY connected
 - e.g., from Internet-facing systems to “disconnected” systems via media (e.g., Stuxnet)
 - “Insider” attacks
 - Compromised account = insider

What can we do to achieve cybersecurity? That is, how do we ensure our mission is not vulnerable to cyberattacks?

The first, obvious approach is to not use any cyber system in our mission because we cannot be sure that a cyber system is ever truly protected from attacks. By eliminating all cyber systems, by definition, our mission cannot be compromised by cyberattacks. On the other hand, this is not always the best approach because cyber systems provide many profits, e.g., automation for efficiency, accessibility, etc.

The second approach is to keep our cyber systems away from the would-be attackers so that they cannot compromise our systems. This is very hard to achieve for two reasons. First, the cyber world is very connected, often in ways that are surprising to users and system administrators, and therefore it is very hard to keep outside attackers from reaching into an internal system. For example, we could disconnect a system from the Internet by not allowing any network connection, but there may still be an indirect way that the system interacts with the Internet, e.g., if the user plugs in a USB thumb drive with data from another computer that was connected to the Internet. The Stuxnet malware that attacked Iran's nuclear capabilities indeed used this method to infect controllers that were not directly connected to the Internet.

Finally, would-be attackers are not necessarily always outside of our organization. There is always the possibility of an “insider” attack by a rogue staff member or volunteer. In addition, if an attacker has already compromised a user account, then he becomes an “insider” because he can now log in as the user.

Achieving Cybersecurity

- Option #3: Be practical (not absolute 0 or 1)
 - *Security* is a state of well-being for information and infrastructures in which the possibility of successful yet *undetected* theft, tampering, and disruption of information and services is kept low or *tolerable*
 - Confidentiality, authenticity, integrity, availability

The practical approach to achieving cybersecurity is to define security not in absolute terms. Instead, we should use the following definition (in fact this is the textbook definition I use in my classes):

Security is a state of well-being for information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or *tolerable*. Security goals include: confidentiality, authenticity, integrity, and availability.

That is, to secure our system means we need to keep the possibility of successful and undetected attacks sufficiently low for our critical missions. In other words, security is about understanding and mitigating risks.

Achieving Cybersecurity

- The security life cycle
 - *Iterations of*
 - Threat and risk analysis
 - Policy decisions
 - Specification
 - Design
 - Implementation
 - Operation and maintenance

Much like how one maintains good health by constantly repeating good habits, achieving cybersecurity requires the constant practice of security process and measures. More specifically, we need to keep iterating the following steps:

- **Threat and risk analysis** – Identify the valuable assets that may be targets of attackers. Identify (new) potential attackers, their motivations, targets and methods. Analyze the likelihood that particular attack will succeed and go undetected.
- **Policy decisions** – Decide the most important assets that we must protect from cyberattacks. That is, decide what risks we cannot tolerate, and what risks we can accept.
- **Specification** – According to the policy decisions, specify which security features are needed.
- **Design** – According to the specification, determine the necessary functionalities of technology components and how they should work together.
- **Implementation** – According to the design, construct the system and test it to verify that it provides the specified and desired features.
- **Operation and maintenance** – Deploy and operate the system according to its intended functions and apply up-to-date patches. Human operators must be trained to properly understand and use the system.

Cybersecurity In Voting Systems

- Threat and risk analysis
 - “Rank order” threats based on
 - Impact, success probability, attribution potential
 - Can a remote attacker change MANY votes?
 - And what are the components that can be targeted?
 - Can a few attackers with access (e.g., posed as worker or voter) change MANY votes?
 - Can a remote attacker shutdown (i.e., make unavailable) the key components (e.g., reporting)?
 - Etc.

Let's discuss the main cybersecurity issues in voting system.

We should follow the security lifecycle, and the first step is threat and risk analysis. We can analyze the threats according to the potential impacts of an attack, its success probability, and our ability to attribute the attack (attribution is a deterrent to a would-be attacker and can reduce the likelihood of an attack).

For example, since the most important “asset” of a voting system is the vote and attackers will attempt to change votes, we can consider:

1. Can a remote attacker – not at the polling station – change MANY votes?

And what are the components that can be targeted in order to do so?

This is the most devastating attack because of the potentially large impact and the difficulty of identifying a remote attacker.

2. Can a few attackers with access (e.g., posing as a worker or voter) change MANY votes?

This attack also can have a large impact, but since it requires physical access, it is more cumbersome for an attacker.

3. We should also consider the availability of the voting and election systems because it affects voter turn-out and is therefore a potential attack target:

Can a remote attacker shutdown (i.e., make unavailable) the key components of the system (e.g., tabulation and reporting)?

Cybersecurity In Voting Systems

- Policy decisions
 - What is really important? Or, what risks can we tolerate (and to what extent) and what can't we?
 - Integrity: votes are accurately counted
 - Voter confidence:
 - Verifiably cast-as-intended
 - Verifiably collected-as-cast
 - Verifiably counted-as-collected

 - *Any* cyberattack can erode voter confidence

The most critical cybersecurity risk in a voting system is that votes are not counted accurately as a result of cyberattacks. Any successful cyberattack, or the belief that a successful attack is inevitable, will erode voter confidence and inflict great harm to our democracy.

All voters deserve to be confident that their votes are counted correctly. For a voter's vote to be counted accurately by the voting system, we need to ensure that the vote is cast in the voting system as intended by the voter, is collected by the voting system as cast, and is counted by the voting system as collected.

Cybersecurity In Voting Systems

- Specification and Design
 - Strong software independent
 - An undetected change or error (including cyberattack) in software cannot cause an *undetectable* change or error in an election outcome; and
 - A detected change or error (due to software) can be corrected without rerunning the election
 - Can recover from cyberattack but requires other trail of evidence (that cannot be affected by the software)

How do we ensure that votes are counted accurately when cyber component(s) are used in the process and we already know that they very likely have security vulnerabilities?

One security feature that a voting system must have is to be “strong software independent.” That is:

- an undetected change or error (including cyberattack) in software cannot cause an undetectable change or error in an election outcome; and
- a detected change or error (due to software) can be corrected without re-running the election.

If a voting system is strong software independent, then it can recover from cyberattacks, but this obviously requires another trail of voter evidence that cannot be tampered or deleted by the software.

Cybersecurity In Voting Systems

- Specification and Design
 - Paper ballots
 - (If done right) Durable evidence to determine correct election outcome
 - Must secure the custody of paper ballots
 - Statistics and auditing
 - Continue to examine random samples of ballots, until
 - There is strong statistical evidence that the election outcome is correct, or
 - There has been a complete manual tally

How do we design a voting system that is strong software independent? We need to maintain voter evidence that cannot be affected by software.

The best approach is to use paper ballots as the durable, independent evidence to verify or determine the correct election outcome, assuming that the paper ballots have accurately captured the voters' intended votes. Obviously, we must also secure the custody of the paper ballots.

With paper ballots, we can:

- apply risk-limited-auditing to verify or determine the correct election outcome;
- continue to examine random samples of ballots and manually count the votes until there is strong statistical evidence that the election outcome is correct, (i.e., the results of manual counting agree with the results of a tallying cyber system), or there has been a complete manual tally. In this case, the tallying cyber system must have functioned improperly either due to a cyberattack or some other error, and we just use the result of the complete manual tally as the correct election outcome.

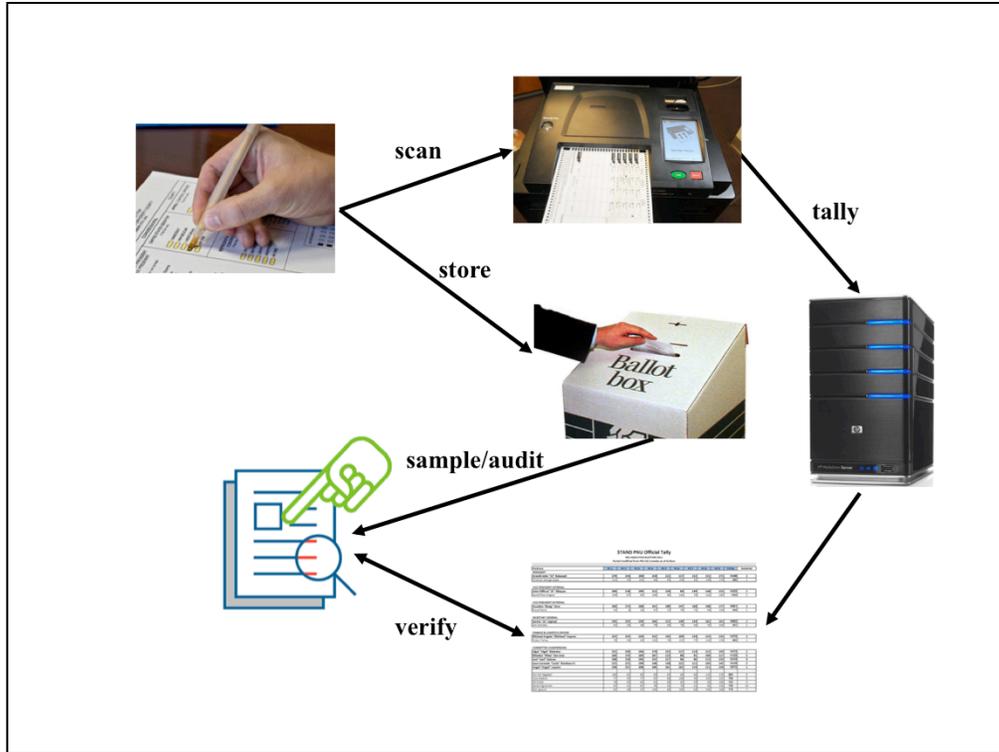
Cybersecurity In Voting Systems

- Specification and Design
 - Paper ballots done right - with auditing, will accomplish:
 - Verifiably cast-as-intended
 - Verifiably collected-as-cast
 - Verifiably counted-as-collected
 - Cannot be completely controlled/manipulated by any cyber component
 - Voters commit/verify votes on ballots
 - Readable/countable by human

How do we ensure that the paper ballots accurately capture voter intent and can be used reliably in an audit?

First, we need to ensure that the voters commit and verify their actual votes on the ballots. **The best approach is to require the voters to hand mark paper ballots that are then scanned and tallied by cyber systems but also dropped in a safe box.** This is because marking each vote captures and verifies the voter's intention in a single act. The much less desirable approach is to have a voter cast his vote on a ballot-marking device, with a cyber component, and print out a paper receipt that the voter would verify and also drop in a safe box. This approach is not secure because the ballot-marking device may have a vulnerability that can be exploited to change votes. Asking the voter to simply read a print-out receipt as verification of his action is an additional step that can be simply ignored by the voter. The difference between these two approaches is critical: with hand-marked paper ballots, a voter both casts and verifies (that is, he verifies as he marks and he cannot cast without already verifying); but with ballot marking devices, he can skip the verification step.

Second, regardless of whether a paper ballot is hand-marked or is a print-out receipt from a ballot-marking device, it must be easily and clearly readable and manually countable. In particular, it must show each and every vote exactly as the voter cast it. It cannot be just a summary of the votes (e.g., that is only a tally, or shows the presidential ballot and omits down ballots). It absolutely cannot be a barcode, QR code, or any other kind of encoding scheme that is readable only by a machine because the cyber system that reads the ballots also can be compromised and lie to the voter or auditor. During a manual review, a human must be able to view evidence of the voter's original act.



This figure illustrates the workflow and summarizes the design of a voting system that is strong software independent, that is, a system that can recover from any cyberattack without the need to re-run an entire election. This is the “gold standard” for voting systems from the point-of-view of cybersecurity researchers and computer scientists who have studied election systems.

A voter is given a paper ballot, he marks the intended vote, then he puts the ballot on a scanner to have the machine record the vote, and once the scanning is done, the voter also drops the ballot in a safe box. The scanning machine forwards the recorded votes to a tallying machine, which counts the votes from all voters and outputs the election result. Auditors may then open the safe box to perform a risk-limiting audit, (i.e., manually read and count samples to verify that the outputs from the tallying system are correct).

Cybersecurity In Voting Systems

- Implementation
 - Not all cyber systems are created equal
 - Choice of hardware and operating system
 - Choice of programming language
 - Secure coding practice
 - Review (open design/source)
 - Penetration testing, bug bounty
 - Latest security technologies
 - E.g., new hardware and software components specifically designed to provide security protection
 - *Don't use the same system for more than a few years!*

There are many approaches to implement the same design, and cybersecurity should be the first consideration when making decisions. Ideally, we should use:

- hardware that provides built-in security support, such as a cryptography engine, trusted platform module, etc.
- operating system that provides the latest security technologies, such as sandboxing, application signing, etc.
- programming language that reduces the chance of programming errors (e.g., buffer overflow) that can lead to security attacks.
- secure coding practice that emphasizes correctness and safety (e.g., always performing bounds check) over efficiency.
- review of design and code that checks security vulnerabilities. When possible, use an open-source system (or components) that can be reviewed by many experts.
- penetration testing to identify potential attacks and, when possible, establish a bug-bounty program to invite experts to test the system.

Technology vendors are always hard at work developing new technologies that provide better security protection. For example, in the past five years, there have been major, generational advances -- not mere updates -- in hardware (with a built-in cryptography engine) and operating systems (with mandatory application signing) that enable systems that utilize these new technologies to be significantly more secure.

Given the importance of cybersecurity, we want our voting systems to be built on top of the latest generations of hardware and operating-system technologies. That is, we should be using the same systems for **no more than five years**.

Cybersecurity In Voting Systems

- Operation and maintenance
 - Adopt best practices in cybersecurity, e.g.,
 - Strong authentication and data encryption
 - Blocking and detecting bad activities at network perimeters as well as endpoints
 - Up-to-date security patches
 - Penetration testing
 - Training, e.g., anti-phishing

Cybersecurity requires constant vigilance at all components and by all parties. That is, we need to always use the best practices:

- Enforce strong authentication, such as two-factor authentication
- Encrypt whenever possible, that is, encrypt all data at rest and all network traffic that does not need to be in the clear.
- Protect both the network perimeter and endpoints, that is, use intrusion prevention and detection systems to block and detect bad activities to the network as well as on endpoint computers.
- Diligently apply up-to-date security patches, in fact, all systems should be set to automatically download and apply security updates.
- Schedule regular penetration testing by third-party providers and make improvements according to findings.
- Perform regular user training (e.g., use training tools to teach users how to identify phishing emails).

In Summary

- Any cyber system is vulnerable.
- “Strong software independent” systems require a human-verifiable element to recover from cyberattack and retain voter confidence.
- Paper ballots are the durable, independent trail of voter intent.
 - Voters hand-mark their paper ballots, submit the paper ballots to the scanning machine, and drop them in a safe box.

Any cyber system is likely to be vulnerable to attacks. For voting systems, a cyberattack can potentially change a very large number of votes and hence the outcome of an election. More importantly, any cyberattack on voting systems, regardless of its real impact, will severely erode voter confidence and affect future voter participation.

Therefore, we need a voting system that can recover from any cyberattack without the need to rerun the election. That is, such a system will give voters the confidence that their votes will never be compromised by cyberattacks. This can be achieved by making the voting system “strong software independent,” which in turn requires paper ballots as the durable, independent trail of voter intent that can be manually audited by humans (through sampling and counting). The gold standard is to have the voters hand-mark their paper ballots, submit the paper ballots to the scanning machine, and once scanned drop them in a safe box. This approach guarantees that the voters verify their intended votes while casting the votes, and the risk-limiting auditing process will guarantee that the votes are collected and counted accurately; that is, this gold-standard approach guarantees that votes by the voters are counted accurately.

Acknowledgement

In this report, I have borrowed important concepts, in particular, “strong software independent,” from the report “Public Evidence from Secret Ballots” (see <https://arxiv.org/abs/1707.08619>). One of the primary authors is Professor Ron Rivest at the Massachusetts Institute of Technology and the “R” of RSA, the most widely-used public-key cryptography algorithm. Professor Rivest is also a winner of the Turing Award, internationally recognized as “Nobel Prize” for computer science.

Basic Security Requirements for Voting Systems

Wenke Lee, Ph.D.

Secure, Accessible & Fair Elections Commission

October 8, 2018

Background

At the SAFE Commission meeting in August, I presented a very simple overview of cyber threats and discussed the design principles for secure voting systems. A copy of that PowerPoint is on the SAFE Commission website with a transcript from the August meeting.

Below, I offer a reference document for all Commissioners, which is: I.) a summary of basic security requirements for a secure voting system, II.) a comparison of the two main approaches under discussion (namely, hand-marked paper ballots vs. a ballot-marking device with paper printouts), III.) a description of the current consensus among computer scientists for a voting system based on hand-marked paper ballots, and IV.) a proposal that the State of Georgia consider cost-effective measures, such as leasing – instead of purchasing – voting machinery.

I. Basic Security Requirements

Strong Software Independent

A voting system must ensure that each voter's vote is counted accurately. That is, the vote is cast in the voting system as intended by the voter, is collected by the voting system as cast, and is counted by the voting system as collected.

The most critical cybersecurity risk in a voting system is that votes are not counted accurately as a result of cyberattacks. Therefore, a voting system must be “strong software independent,” that is:

- an undetected change or error (including cyberattack) in software cannot cause an **undetected** change or error in an election outcome; and
- a detected change or error (due to poor software performance or cyberattack) can be corrected without re-running the election.

The only way to achieve “strong software independent” status is for the voting system to maintain a trail of voter evidence that cannot be tampered or deleted by **any** software component (including data within a device, data in transit, and data at rest on a server).

Continued...

Paper Ballots

A voting system must use paper ballots as the durable, independent evidence to verify or determine the correct election outcome, by ensuring that the paper ballots have accurately captured the voters' intended votes and that the custody of the paper ballots is secure.

With paper ballots, we can apply risk-limited-auditing to verify or determine the correct election outcome, that is, we can continue to examine random samples of ballots and manually count the votes, until:

- there is strong statistical evidence that the election outcome is correct, (i.e., the results of manual counting agree with the results of a tallying cyber system), or
- there has been a complete manual tally. In this case, the tallying cyber system must have functioned improperly either due to a cyberattack or some other error, and we turn to the complete manual tally as the correct election outcome.

In order to support risk-limited-auditing, paper ballots must be easily and clearly readable and manually countable. In particular, a paper ballot must show each and every vote exactly as the cast by the voter. It cannot be just a summary of the votes (e.g., only a tally, or only the presidential ballot and not the down ballots). A manual count absolutely cannot rely upon a barcode, QR code, or any other kind of encoding scheme that is readable only by a machine because the cyber system that reads those codes also can be compromised and lie to the voter or auditor. In short, during a manual review, a human must be able to clearly see evidence of the voter's original act.

II. Hand-Marked Paper Ballots vs. Printouts from a Ballot-Marking Device

In order to ensure that paper ballots accurately capture voter intent, **the best approach is to require the voters to hand mark paper ballots that are then scanned and tallied by cyber system but also dropped into a safe box.** This is because marking each vote captures and verifies the voter's intention in a single act.

The much less desirable approach is to have a voter cast his vote on a ballot-marking device, with a cyber component, and print out a paper receipt that the voter would verify and also drop into a safe box. This approach is not secure because the ballot-marking device may have a vulnerability that could be exploited to change votes. Asking the voter to read a printout receipt as verification of his/her action is an additional step that simply could be ignored by the voter.

The difference between these two approaches is critical: With hand-marked paper ballots, a voter both casts and verifies (that is, the voter verifies as s/he marks and cannot cast without already verifying). However, with ballot marking devices, the voter can easily skip the verification step.

III. Consensus Opinion Among Computer Scientists

A steady stream of election security studies by independent, non-profit and/or academic researchers has been produced in the past decade, and especially during the past two years.

These studies offer what is now a well-developed consensus from cybersecurity researchers and computer scientists across the United States who agree that a secure voting system should work as follows:

1. A voter is given a paper ballot.
2. S/he marks the intended vote.
3. S/he then puts the ballot on a scanner to have a machine record the vote.
4. Once scanning is done, the voter also drops the ballot into a safe box.
5. The scanning machine forwards the recorded votes to a tallying machine, which counts the votes from all voters and outputs the election result.
6. Auditors may then open the safe box to perform a risk-limiting audit, (i.e., manually read and count samples to verify that outputs from the tallying system are correct).

See “Additional Sources & Studies” at the end of this document for links to studies and handbooks for election officials.

At the 2018 Georgia Tech Cybersecurity Summit (held on October 4, 2018), Mr. Michael Morell, former acting director of the CIA, told the audience that our “failures to imagine” how our adversaries would attack us have been our biggest and most devastating failures as a nation (e.g., the 9/11 terrorist attack and the DNC server hack, to name two). Therefore, we must take the threat of cyberattacks against voting systems very seriously even though there is not yet proof that past cyberattacks have affected any election outcome in the United States.

Mr. Morell also revealed that, at the CIA, the top most secret information is now held on paper only; he said, “We are going back to paper.” Therefore, given that we must protect the integrity of votes, requiring voters to hand-mark and verify votes on paper ballots is the most prudent approach.

IV. Additional Security and Fiscal Considerations: Leasing & Print-on-Demand

Given the importance of cybersecurity, a voting system must use the latest generation of hardware and operating-system technologies, many of which are designed to provide stronger security protection than the previous generations of such technology. Instead of purchasing a system and using it for nearly 20 years, the State of Georgia should consider leasing a voting system, for example, every five years or less. This helps to ensure that Georgia uses the most up-to-date technology available. It also applies pressure to vendors to keep their products up-to-date. The option of lease vs. purchasing also alleviates the need for the State of Georgia to appropriate such a dramatic volume of funds (estimated to be \$30M - \$100M+) at one time for the purchase of a voting system.

At the August 2018 public meeting of the SAFE Commission, we heard that other areas of the country have effectively used print-on-demand features to reduce the cost of paper ballots. A cited example was that of King County (metro Seattle) – an industrious area that includes metropolitan Seattle and the headquarters of technology leaders Amazon and Microsoft. Of note is that King County reduces paper waste and the financial cost of unnecessarily printed,

paper ballots by equipping polling stations with an electronic copy of an official, certified paper ballot. Such an approach in the State of Georgia would allow the Secretary of State's office to certify the official ballot for each County, provide a human-readable copy for reference by poll workers, and provide an electronic copy for print-on-demand as voters arrive. A print-on-demand approach alleviates the financial and logistical burden of providing thousands of paper ballots (which may go unused) to 159 counties.

Summary

We need a voting system that can recover from any cyberattack without the need to rerun the election. Such a system will give voters the confidence that their votes will never be compromised by cyberattacks. This can be achieved by making the voting system "strong software independent," which in turn requires paper ballots as the durable, independent trail of voter intent that can be manually audited by humans (through sampling and counting). Paper ballots must be easily and clearly readable and manually countable; a paper ballot must show each and every vote exactly as the voter cast it.

A secure voting system should use hand-marked paper ballots instead of ballot marking devices. That is, voters hand-mark their paper ballots, submit the paper ballots to the scanning machine, and once scanned drop them into a safe box. This approach guarantees that the voters verify their intended votes while casting the votes, and the risk-limiting auditing process will guarantee that the votes are collected and counted accurately. This consensus approach among the cybersecurity research community ensures that votes by the voters are counted accurately.

Instead of purchasing a voting system that is used for many years, the State of Georgia should lease a new system every few years to ensure its voting system is built on top of the latest generation of security technologies provided via the latest hardware and operating systems.

Acknowledgement

I have borrowed important concepts, in particular, "strong software independent," from the report "Public Evidence from Secret Ballots" (see <https://arxiv.org/abs/1707.08619>). One of its primary authors is Professor Ron Rivest at the Massachusetts Institute of Technology and the "R" of RSA, the most widely-used public-key cryptography algorithm. Professor Rivest is also a winner of the Turing Award, internationally recognized as the "Nobel Prize" for computer science.

For Reference

Questions to Ask Potential Vendors

At the August meeting, vendors expressed a willingness to customize a secure voting solution for the State of Georgia. In addition to the Request for Information by the Georgia Secretary of State's office (dated Aug. 20, 2018), worthwhile questions surrounding cybersecurity to ask a prospective voting or election system vendor are:

- What internal cybersecurity practices do you follow within your organization? How do those compare to the standards recommended by the National Institute of Standards and Technology at the U.S. Dept. of Commerce?
- What cyberattack(s) has your organization experienced in the past 24 mos., and how were they managed?
- What is your process for identifying new cybersecurity threats to your products? How are those cyber vulnerabilities managed and rectified? How are they reported to prior customers?
- What percent of your product was developed in-house by your organization? Which portions were developed by sub-vendors?
- How are sub-vendors involved in cybersecurity updates (i.e., code, patches, controls, etc.)?
- How will you collaborate with the State of Georgia to mitigate any security risks that we identify, as well as respond to a unique cyberattack in Georgia involving your product?
- When was your product launched? When was it last updated? When do expect to perform the next significant update to this technology?

Recommended Requirements of Vendors

per guidance by the Harvard Kennedy School Belfer Center for Science and International Affairs

IDENTIFY

- **Examine all the possible functionalities of the device** and of any of its subcomponents. Specifically pay attention to the wireless and networking functionality.
- **Know the certification status of all your equipment.** The Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG) provides federal level certification standards. Many states have their own certification process.

PROTECT

- **If you have a DRE machine that does not produce a paper trail, you should either replace the device or purchase an add-on (VVPAT adapter) that creates a paper trail.**
- **Physical Security/Access Seals.** Use serialized tamper-evident security seals and chain of custody logs to limit physical access to voting machines and track whenever removable media is plugged into the scanners.
- **Penetration test systems.** Conduct, or hire a third-party firm to conduct, a source code audit and penetration test of all vote-casting devices.
- **Restrict device functionality to what is required.** Even if you have disabled a feature through a settings page (such as Wi-Fi connectivity), those features could still be

exploited. You should not trust that toggling a switch in software actually will disable the functionality. If possible, the hardware should be removed.

- **Isolate the device from external connectivity. Do not connect the device to a network, which includes not using a cellular modem.** If network connectivity cannot be avoided, make sure to keep the network connection disabled until you intend to transmit the results.
 - **Create a copy of the results** (either a printout or by saving it to removable media) before you connect to the network.
- If removable media is used to transfer data (e.g., ballot definition files, vote tallies):
 - **Have a procurement strategy for devices.** Purchase physical media devices directly from a trusted vendor and obtain assurance that the suppliers from whom your vendors procure their memory can also be trusted. If you must use devices from an unverified source, obtain them from a location that you would not otherwise use, to make it less likely that a bad actor could plant USB devices that could infect your systems.
 - **Protect device chain of custody.** Once devices are procured, ensure that they are stored securely and access is limited to the appropriate audience. When in use, maintain a physical record of the device—including where the device has been and who has been in contact with it— to limit the opportunity for manipulation.
 - **One-way/one-time use:** Only use physical media once, from one system to a second system, then securely dispose of it. A USB device could either (1) transfer data from one air-gapped machine to another or (2) transfer data from an air-gapped machine to an outside one prior to disposal, but not both. When feasible, use write-once memory cards or write-once optical disks instead of USB devices. This ensures one-time use is self-enforced by the technology.
 - **Scan media devices** for malware. If you detect abnormalities, don't use the device and contact forensic experts for assistance.

DETECT

- Perform logic and accuracy testing of the programmed device.
- Verify the seals and chain of custody logs via a unique identifier (e.g., seal number).

RESPOND & RECOVER

- Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Continued...

VENDOR CONSIDERATIONS

- Vendors are integral to vote casting devices as every device has been physically constructed, programmed, and is often maintained by various vendors. A compromise or oversight at any of these points would allow an attacker to change or erase election results.
- See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in [Appendix 1: Vendor Selection and Maintenance](#).

Additional Sources & Studies

- Center for Election Innovation & Research. September 2018. *Voter Registration Database Security*. Washington, DC: CEIR. <https://electioninnovation.org/2018-vrdb-security/>
- National Academies of Sciences, Engineering, and Medicine. September 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. <http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25120>
- DEF CON Voting Village 26. September 2018. *Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*. Las Vegas: DEF CON. <https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf>
- Harvard Kennedy School Belfer Center for Science & International Affairs. February 2018. *Defending Digital Democracy: The State & Local Election Security Playbook: Technical Recommendations*. Cambridge, Mass.: Harvard Press. <https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook>
- Center for Internet Security. February 2018. *A Handbook for Elections Infrastructure Security*. East Greenbush, NY: CIS. <https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>
- *Public Evidence from Secret Ballots*. In Proceedings of the Second International Joint Conference for Electronic Voting (E-Vote-ID), October, 2017. Lecture Notes in Computer Science 10615, Springer. Also available at <https://arxiv.org/abs/1707.08619>

###

Addendum to Basic Security Requirements for Voting Systems

Wenke Lee, Ph.D.
Secure, Accessible & Fair Elections Commission

January 3, 2019

Background

Before the SAFE Commission meeting on December 12, 2018, I distributed a reference document to all Commissioners, which was: I.) a summary of basic security requirements for a secure voting system, II.) a comparison of the two main approaches under discussion (namely, hand-marked paper ballots versus a ballot-marking device with paper printouts), III.) a description of the current consensus among computer scientists that a voting system should be based on hand-marked paper ballots, and IV.) a proposal that the State of Georgia consider cost-effective measures, such as leasing – instead of purchasing – voting machinery.

Based on our discussions at the meeting and feedback from citizens, I would like to provide an addendum to that reference document, which includes: I.) a discussion of the requirements for a pre-certification audit following an election and the shortcomings of paper receipts from ballot-marking devices (BMDs), II.) a brief discussion that cybersecurity is always a central concern even with future technologies, III.) and clarification of a misunderstanding about election and voting system security.

I. Post-Election Audit: Avoid “Garbage-In, Garbage-Out”

At the SAFE Commission meeting in December, many Commissioners, as well as employees of the Secretary of State’s Office, expressed support for the implementation of a formal election audit process. The purpose of a pre-certification election audit is to verify that the votes cast by voters are accurately captured and counted. The audit must verify the reported results, rather than merely test how the voting system performed. In the context of our current election system where votes are tallied by computers, an election audit can verify that automatically tallied results are correct prior to certification of the results – but only if a paper record exists.

A voting system must provide either a **human readable, post-vote paper receipt from a ballot-marking device** or an **actual paper ballot** as the durable, independent evidence that can be used as the authoritative source document in an audit or recount. Further, the paper record must have accurately captured the voters’ intended votes, and the chain of custody of that paper must have remained secure after the ballots were cast by voters.

In order for paper receipts from a ballot marking device (BMD) to be useful in an audit, all of the following conditions must be met:

- 1) ALL voters must be WILLING to verify that each and every single vote that s/he cast with a BMD is clearly printed on the paper;
- 2) ALL voters must be ABLE to verify that each and every single vote that s/he cast with a BMD is clearly printed on the paper;
- 3) ANY voter who discovers a discrepancy is ENCOURAGED to speak up and BE ALLOWED TO VOTE AGAIN.

Unfortunately, to date, there is no systematic user study that has demonstrated that these conditions can be met. Quite to the contrary, studies and observations at polling stations have thus far suggested that a large percentage of voters do not carefully look at the printouts to verify that their votes have been printed on the paper correctly. Further, many voters cannot detect the discrepancies between votes they have cast with a BMD and errors on the printouts, especially for “down-ballot” races. And some voters do not feel comfortable to speak up if they discover a discrepancy, perhaps because they think such a discrepancy should not have happened so it must be their own fault. Some, wanting to maintain their right to a secret ballot, hesitate to disclose to poll workers who they intended to vote for and the specifics of the error.

These findings are not surprising at all because of human nature – not all of us are as diligent as we should be, many of us do not have the required memory capacity to remember all the votes we cast, and some of us would be embarrassed to inconvenience poll workers and fellow voters by asking to vote again.

In addition, it should be clear that it is not sufficient to have only some voters who are willing and able to verify their paper receipts. If receipts with erroneous votes are not identified (because some voters are not willing or unable), the post-election audit or recount will not produce an accurate result of votes cast by voters; and therefore, all voters are ultimately affected. For example, the audit may just confirm the tallied result from the voting system, which is incorrect because the BMDs had registered the votes incorrectly in the first place.

In summary, it is meaningless to perform a post-election audit on printouts that cannot be guaranteed to be valid in the first place; the audit would just be “garbage-in, garbage-out,” and perhaps worse, give a false sense of accuracy or legitimacy of the election results.

Therefore, I believe it would be unwise, from a return-of-investment point of view, for the SAFE Commission to recommend that Georgia spend tens of millions of dollars to purchase a new voting system when, compared with the current system, the only major new feature would be paper receipts that cannot even be guaranteed to be valid and cannot be realistically audited.

Instead, once again, I recommend that we use the most accurate, safest, and most secure approach, which is to require a voter to hand mark his/her paper ballot, scan it, and drop it in a safe box. This is the most accurate method for voting because with hand-marked paper ballots, a voter both casts and verifies as they mark; it happens naturally and therefore human discipline and short-term memory play no role. This is the safest and most secure record for an audit because hand-marked paper ballots in a safe box have not been processed by any cyber

system and would not be vulnerable to any possible cyberattack. Although computerized scanners and tabulators are at risk of cyberattacks or errors, secure hand-marked paper ballots remain as the authoritative, auditable source documents for verifying computer-tabulated results. If errors are identified, paper ballots can be hand counted and the accuracy of the votes ultimately assured. That is not the case with BMDs: no authoritative hand count can be accomplished using BMD printouts that many voters are not able to verify.

Arguments for BMDs have been vocal and will likely continue. I recommend that we require vendors to provide evidence based upon rigorous, scientific studies that prove how BMD paper receipts would meet the requirements of a pre-certification election audit before they market their BMDs to Georgia. A rigorous study must involve a large number of representative, average voters using a mocked, complete ballot (i.e., including all, top to bottom, ballot races) similar to one from a recent major election, and must include printouts with erroneous votes (unknown to test subjects) to observe how willing and accurately voters will verify their votes. I also recommend that our decision-makers (e.g., legislators and state and county election officials) conduct similar rigorous studies using a proposed BMD system before they decide to purchase/deploy.

Further, even if BMDs are used, policy makers will need to plan for required feedback and mitigation procedures when voters identify BMD malfunction or errors. Is the equipment taken out of service? Are back-up units moved into place and planned for in the budget? Are paper ballots used from that point on?

All voters have the right to expect that their votes will be counted accurately. For a post-election audit or recount to be valid, all voters must have successfully verified that their votes have been accurately recorded on paper. If BMDs are used, the voters are in effect being required to use their memory skills to verify that BMDs did not make any errors. Why should voters be burdened to check the accuracy of voting systems? Isn't it the responsibility of the election officials and vendors to provide the appropriate systems and procedures to ensure that all votes will be counted accurately? More importantly, how do we guarantee the voting rights of all voters, regardless of their disabilities? In particular, if BMDs are used, how could we accommodate the large numbers of voters who do not have the memory skills to verify complex ballot content?

II. Future Technologies: Integrity/Security Is the Invariant

It always is dangerous to predict the future: who would have thought that we would be discussing a return to paper ballots in 2018? But we are here because of concerns about cybersecurity and its impacts on election integrity. Cybersecurity will be a constant concern, regardless of future technologies, and the likelihood of its manifestation will evolve with technology.

For example, it is tempting to think that in the near future we will adopt Internet-based (online) voting because young people simply will demand it. However, even if we can completely solve the user authentication problem to protect ballot secrecy, it is very challenging to guarantee

that a vote from a computer on the Internet is not the result of voter coercion/intimidation, vote buying, or malicious altercation.

On the other hand, we should have faith in our younger generations that -- despite their propensity for doing more and more activities online -- they will go to polling stations once they are educated about both a.) the importance of participating in our democracy and b.) the cybersecurity and vote integrity risks to online voting. Evidently, the very few countries that have experimented with allowing online voting have not seen an increase in voter participation (that is, there is no evidence that it enables more people to vote or satisfies a new voter preference). In fact, engaging with others at a physical polling place may actually promote a sense of pride and camaraderie among the public.

III. The System Is Not Connected to the Internet but It Can Still Be Hacked

It is easy to mistakenly believe that cybersecurity is all about Internet-facing security because after all, today most cyberattacks are coming from the Internet. However, as long as a computer accepts input data from another device (software or hardware) that is or has been part of an Internet-connected network, it can still be hacked via the Internet. For example, when an Internet-facing system is compromised, malware can embed itself in PDF, Word, and Excel files on the system, and these documents can eventually be loaded to a USB thumb drive. If this thumb drive then is used to share files among computers that are disconnected from the Internet, those computers can be infected by the same malware.

In fact, that is how advanced persistent threats (APTs) work: compromising an Internet-facing system, then leveraging data as it is transmitted to internal systems (e.g., via email or portable medium such as USB thumb drives) to infect greater parts of the system. A real-life example is the Stuxnet virus, which was able to infect controllers of Iran's nuclear machinery even though those controllers were not directly connected to the Internet or other networked computers.

In the context of election and voting systems, a ballot-marking device needs to be loaded with ballot data using a voting system memory card. The ballot data is formulated on another computer system, which is based on original data/documents, e.g., voter registration files and ballot programming files, that at some point came from an Internet-facing system. Therefore, even though a BMD or voting machine is not directly connected to the Internet, it still is under the threat of cyberattacks from the Internet or by individuals who have direct access to the computers.

Finally, we should not make the "failure to imagine" mistake again. We, as a nation, have failed to imagine how cyberattackers would manipulate our defense, healthcare, credit bureaus, and social media systems for malicious gain. Researchers already have demonstrated attack methods that can change votes recorded by a DRE or BMD. It requires no imagination to know that real attackers will try similar attacks on our election and voting systems. In the history of cybersecurity, researchers have tried to discover vulnerabilities, demonstrate new attacks, and urged vendors/industry to fix their vulnerable systems or practices. In the many cases where

responses by vendors/industry were not adequate, we ultimately have seen real attacks eventually surface and create havoc.

Summary

In order to ensure that an election and an audit is meaningful and accurate, we must have paper ballots that accurately capture the votes cast by voters. This in turn requires that, *if* BMDs are used, *all* voters are willing and able to verify a paper receipt (that is, a 100% voter compliance would be required). Studies thus far have shown that many voters are not willing or not able to do that, and it is unlikely that human nature can be changed. Therefore, printouts from BMDs cannot be used to guarantee a correct election or audit result. We should instead rely upon hand-marked paper ballots.

Cybersecurity will always be a central concern of voting systems. Never should convenience outweigh the need for better cybersecurity because without cybersecurity, there will be no election integrity.

We must secure all elements of the election and voting systems because even when a system is not directly connected to the Internet it can still be attacked by those who have direct access or via data that can be traced back to an Internet-facing system.

Lynn Bailey
Elections Director, Richmond County, Georgia
SAFE Commission Member

It has been my privilege to serve as Elections Director in Richmond County these past 25 years and my absolute honor to serve as a member of the SAFE Commission established by former Secretary of State Brian Kemp and charged with researching and evaluating a new voting system for the State of Georgia. The Commission was also asked to solicit feedback, perform a cost analysis, research post-election audit procedures and provide legislative recommendations to lawmakers.

Members of the Commission heard from experts who provided an overview of Georgia's current voting system, the procurement process used by the State, and other legal matters for consideration when implementing a new system. We also heard from expert panelists on topics such as voting rights, security, voting accessibility, intergovernmental coordination between counties and the state. During the process, Commission members were given an opportunity to provide input and to ask questions. Members of the Commission had numerous opportunities to speak with voting equipment vendors and to participate in a public demonstration of the equipment.

As background, I was responsible for the administration of a paper ballot system from 1993 through 2002, at which time the state converted to the electronic system currently used in Georgia. With that background in mind, I do have valid concerns about the manual issuance of paper ballots both during Advance Voting and on Election Day. Advance Voting, which was implemented in Georgia for the first time in 2003, is a very popular option for Georgia voters with as many as half of the voters who participate in any given election choosing to cast their ballot during Advance Voting.

If moving to an all paper ballot system, each Advance Voting center must be equipped to provide a paper ballot for any registered voter of the jurisdiction and poll workers would be required to manually select the proper ballot for each and every voter who casts a ballot. In our jurisdiction of 123,000 registered voters, that equates to 68 different ballot styles in any county-wide election and 204 ballot styles during a Primary. In larger jurisdictions and in jurisdictions where bi-lingual ballots are mandated, even more ballot styles would be required. Printing ballots on demand using a printer in the polling site would help with printing costs, but would not mitigate the risk of a poll worker inadvertently issuing the wrong ballot to a voter. The same scenario exists for Election Day voting in many counties. Election Day polling sites across the state could have as few as 1 ballot style or as many as 30, or more.

As a part of my personal preparation, I offered a survey to election officials across the state seeking their input on their preferred method or type of voting system using the three methods stated in the Request for Information issued by the State of Georgia as a basis. The methods are: (1) paper balloting, (2) ballot marking device for all in person voting, or (3) a hybrid system using paper balloting for mail and Election Day voting and ballot marking devices for Advance Voting.

There were 76 responses to the survey and 95% of those who responded chose Method 2 - using ballot marking devices for all in person voting including Advance Voting and Election Day voting.

Number of Registered Voters	Number of Respondents	*Method Preference	Estimated Printing Cost for all paper
1,000 - 10,000	21	0 - Method 1 20- Method 2 1- Method 3	\$1,000 - 10,000
		95% prefer Method 2	
11,000 - 40,000	25	2 - Method 1 23 - Method 2 0 - Method 3	\$4,000 - 40,000
		92% prefer Method 2	
42,000 - 100,000	17	0 - Method 1 17 - Method 2 0 - Method 3	\$15,000 - 58,000
		100% prefer Method 2	
105,000 - 300,000	8	1 - Method 1 7 - Method 2 0 - Method 3	\$75,000 - 165,000
		87% prefer Method 2	
450,000 +	5	0 - Method 1 5 - Method 2 0 - Method 3	\$200,000 - 500,000
		100% prefer Method 2	

*Method 1 - all paper balloting
 Method 2 - ballot marking device for all in-person voting
 Method 3 - paper balloting for Election Day and by mail and ballot marking device during Advance Voting

Based on the information provided to the Commission, research, presentations, public input and personal experience, I submit the following recommendations for what I believe would be the best solution for a new voting system for Georgia that contemplates both the ease of use by voters and effective and secure election administration.

Voting System Recommendations

1. During Advance Voting, I do not recommend paper balloting or any other voting method or system that is dependent upon the manual issuance of ballots by poll workers. This same thought applies to Election Day voting in polling places where multiple ballot styles are required.

2. I fully support post-election audits using a method that takes into consideration the time period for certifying election results and Georgia's runoff election schedule. The auditing process should be transparent and open to the public in the same manner as pre-election testing is now and should allow for monitors in the same way as monitors are now allowed during the early tabulation period for absentee ballots.
3. I do not believe the use of a QR code or a bar code on the voter verifiable paper ballot is a security risk nor do I believe it to be an impediment to our ability to accurately tabulate the voter's choices. I believe that a prescribed high standard of physical security and chain of custody documentation combined with thorough and transparent pre-election testing and post-election auditing procedures will work together to ensure without a doubt that all ballots were accurately tabulated, that the equipment used has performed properly and has not been tampered with, and, will readily identify any possible malfunction or deficiency.
4. Any manipulation of the software used in any voting system should be easily detected by the administrator and security should be practiced and evaluated on a regular basis.
5. Any system should have robust capabilities for in-person voting by voters with disabilities including, at a minimum, Braille instructions on the keypad, a good audio system and headset, the ability to enlarge text and change the contrast on the display.
6. Software for bi-lingual ballots should provide the flexibility of adapting to accommodate local dialects.
7. Voters should be able to vote with relative ease.
8. The voting equipment should not be too heavy, should be sturdy, and be easily maintained.
9. Georgia's contract should provide the ability to update software or equipment to keep up with new technology.
10. Counties should have the ability to purchase additional equipment using the pricing structure negotiated in the State contract.
11. Any system purchased should include all components necessary for proper storage and transportation of equipment and also for electronic poll book and ballot on demand printing system as these are critical components of any system regardless of the method used.
12. Legislative changes should include authorizing pilot programs during the November 5, 2019 to assist the State in refining processes prior to the 2020 Election cycle.

I appreciate the opportunity to serve Georgia in such a meaningful way and I look forward to the implementation of our new system. Thank you for the opportunity. It has been my pleasure.

Minority Report

To: SAFE Commission Members

From: Senator Lester Jackson, Representative James Beverly, Michael Jablonski

Subj: Response for inclusion in the final SAFE Commission Report

EXECUTIVE SUMMARY

The Secure, Accessible, & Fair Elections (SAFE) Commission was established in April 2018 with the laudable goal of providing expert advice to the Georgia General Assembly related to the replacement of Georgia's ageing voting system. To that end, its stated mandate was as follows:

The SAFE Commission will conduct thorough discussions on all options – including the feasibility of using all hand-marked paper ballots to all electronic machines with a voter-verified paper trail – and travel the state to solicit feedback from stakeholders. Members will conduct cost analysis of market options, research post-election audit procedures, and provide legislative recommendations to lawmakers before the next session of Georgia's General Assembly.¹

Even under this limited directive, the draft report distributed on January 9 made it clear that the work of the Commission did not meet the aspirations set out for it.²

The problems are multifold:

1. Information on voter-favored hand-marked paper ballots was based on 20-year-old experience, ignoring modern technology developments and the experience of states who have already undergone this exact transition;
2. The Commission ignored the advice of its cyber-security expert regarding the inherent vulnerability of all computer-based voting;
3. The Commission failed to investigate the challenges and problems presented by the machines in the 2018 election, nor was an evaluation on the election initiated; and
4. The Commission failed to establish standards that the General Assembly can use to make its own independent assessment.

This minority report will attempt to address each of these shortcomings. We discuss areas of inquiry that were not adequately covered by the work of the commission. We provide evidence

¹ "Secure, Accessible, & Fair Elections Commission," at http://sos.ga.gov/index.php/elections/secure_accessible_fair_elections_safe_commission, accessed Jan. 13, 2019.

² Draft Secure, Accessible, & Fair Elections (SAFE) Commission Report, January 9, 2019. An April 2018 United States Government Accountability Office (GAO) study on the same issue suggests some critical omissions in the Commission's mandate. See "Elections: Observations on Voting Equipment Use and Replacement," United States Government Accountability Office, April, 2018. In particular, the federal study noted the importance of meeting local voting system standards and of the "the ability to maintain equipment and receive timely vendor support." The Commission never established standards, and did not address vendor support at all. It is an unfortunate omission of the Commission staff that it failed to distribute such a salient document to its members, since this comprehensive study would have been an extraordinarily useful reference for members.

rebutting some of the assumptions and conclusions of the majority report. We also highlight areas of agreement, where we believe the Commission report provided valuable proposals for legislative changes to Georgia election law. Finally, we propose standards for consideration by the Georgia General Assembly in assessing next steps in the process to replace our sadly outdated, insecure voting system.

BALLOT SECURITY

Ballot and system security are the *sine qua non* for election integrity. Indeed, the acronym of the SAFE Commission itself reflects this strong emphasis on the security of our vote. However, the Commission refused to adopt many of the recommendations of the Commission's own appointed cybersecurity expert, Dr. Wenke Lee.³ Dr. Lee's conclusions reflected similar concerns and recommendations to those offered by the nonpartisan election integrity group Verified Voting as well as a consortium of twenty-four national leaders in cyber-security and election integrity. These groups all agreed that the Commission-recommended voting medium, Ballot Marking Devices (BMDs) "share the pervasive security vulnerabilities found in all electronic voting systems, including the insecure, paperless DREs in current use statewide."⁴ An electronic system is vulnerable to a system-wide failure or cyberattack, while hand-marked paper ballots would have to be tampered with one by one.

While the Commission draft report notes Dr. Lee's points, it minimizes them both by suggesting that only Dr. Lee holds these concerns, and by citing only a single argument, that of verifiability.⁵ In fact, the primary argument against BMDs is that, like DREs, they are vulnerable to cyber-attack.⁶ Indeed, the National Academies of Science, Engineering and Medicine note that "Malware—malicious software that includes worms, spyware, viruses, Trojan horses, and ransomware—is perhaps the greatest threat to electronic voting."⁷

"VERIFIABLE" PAPER BALLOT RECEIPT

The fact that BMDs produce a paper receipt recording voter choices is said to ameliorate cybersecurity risks. Dr. Lee's paper, however, highlights why this argument fails: the paper receipts provided by ballot marking devices are not, in practice, verified by voters, and in fact it is extraordinarily difficult to do so.⁸ This point has also been made by the National Academies of Science, Engineering, and Medicine: "Unless a voter takes notes while voting, **BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent.**"⁹ [emphasis added] A simple exercise would demonstrate this point—we would encourage members of the Georgia legislature to review a mock-up ballot

³ See, e.g., "Georgia panel backs new voting machines over hand-marked paper ballots," Mark Niese, [The Atlanta Journal-Constitution](#), Jan. 10, 2019; see also, "Commission recommends machine-marked ballots for Georgia," Kate Brumback, [Washington Post](#), Jan. 10, 2019.

⁴ Letter from Dr. Dr. Mustaque Ahamad, Professor of Computer Science, Georgia Institute of Technology, et al., Jan. 7, 2018.

⁵ Draft Secure, Accessible, & Fair Elections (SAFE) Commission Report, Jan. 9, 2019, pp. 14-15.

⁶ "Addendum to Security Requirements for Voting Systems," Dr. Wenke Lee, Jan. 3, 2019.

⁷ [Securing the Vote: Protecting American Democracy](#), National Academies of Science, Engineering, and Medicine, 2018, p. 86.

⁸ "Addendum to Security Requirements for Voting Systems."

⁹ [Securing the Vote: Protecting American Democracy](#), p. 79.

with a similar number of races and ballot initiatives as the 2018 general election, and then review a mock paper receipt similar to what each vendor would produce, to test whether in fact a voter could recall all of the races and votes on ballot initiatives as they appear. Despite this concern, however, the Commission failed to provide any guidance or standards with regard to what sort of paper receipt or full-face ballot should be required for Georgia's next voting system--suggesting that a practically unverifiable summary sheet is equally acceptable as a full ballot.

FAILURE TO EVALUATE HAND-MARKED PAPER BALLOTS

The Commission report, under recommendation number 6, provides a number of critiques of paper ballots and arguments supporting BMDs. All of these critiques, however, are based on Georgia election officials' experience of two decades ago. The Commission did not provide any information to the members on modern technology and usage. This one-sided evaluation appears custom-designed to result in a predestined recommendation. Two of the purported shortcomings are listed below, along with counter-evidence that was not presented to Commission members.

Residual Votes

One of the primary complaints with regard to paper ballots is the residual vote rate--i.e., the number of over- or under-votes in ballots. The Commission report notes with concern that paper ballots resulted in a high number of undervotes, particularly in jurisdictions using optical scanners.¹⁰ This analysis, however, is based on Georgia's much earlier experience in using paper ballots, up to and including the 2000 elections, when counties scanned ballots centrally. Centralized scanning does not allow the voter to be notified of a residual vote, nor does it allow for a voter to correct a ballot containing such an error. This stands in contrast to the precinct-based scanning that is currently being contemplated.

There has been a great deal of scholarship comparing residual votes across different voting systems, and none of this was provided to Commission members to help them evaluate systems on an equal footing. In both Florida and Michigan, residual vote rates have been documented at less than 1% in those jurisdictions where optical scanners were utilized at the precinct directly, rather than centralized at the county level.¹¹ A later study conducted by Massachusetts Institute of Technology Professor Charles Stewart found that, in terms of residual votes, there was no meaningful difference in jurisdictions that utilized DREs compared to those that used hand-marked paper ballots and optical scanner at the precinct level.¹² The main substantive difference that voters encountered between voting methodologies was wait time; voters who utilized DREs generally had to wait significantly longer to cast a ballot than those who cast paper ballots.¹³

¹⁰ Draft Secure, Accessible, & Fair Elections (SAFE) Commission Report, Jan. 9, 2019, p. 9.

¹¹ "Losing Fewer Votes: The Impact of Changing Voting Systems on Residual Votes," Michael J. Hamner et al., Political Research Quarterly, Vol. 63, No. 1, March 2010, p. 134.

¹² "Election Technology and the Voting Experience in 2008," Charles Stewart III, The Massachusetts Institute of Technology, Draft of March 25, 2009, found at <http://web.mit.edu/supportthevoter/www/files/2013/09/Election-Technology-and-Voting-Experiences-in-2008.pdf>.

¹³ Id.

Furthermore, there is significant evidence of anomalous residual votes in the 2018 general election Lieutenant Governor’s race—undervotes that occurred solely on votes cast on machines, and not paper.¹⁴ Until these problems can be properly identified, it seems premature, at best, to be recommending another computer-based voting system that share the same cyber-security vulnerabilities as the machines that demonstrated significant problems a mere two months ago.

Ease of Administration

Another argument promoting a BMD system suggested that both voters and election officials would have an easier time adjusting to another touch-screen, computer-based system.¹⁵ The Commission report’s evidence was based on voter surveys following a pilot program utilizing ES&S BMDs and discussions with county officials. However, other states have moved from DREs to hand-marked paper ballots with precinct-based scanners, and report little trouble with the transition: Maryland made this transition in 2016, and reported that “the deployment of the new equipment in the 2016 general election went smoothly with no significant challenges.”¹⁶ Neither recent studies nor election officials who have already undertaken this transition were consulted by Commission members to allow them to evaluate different options on a level playing field. There is no reason to believe that Georgia voters or polling officials are somehow less capable than those in Maryland or other jurisdictions that have made this transition from DREs to hand-marked paper ballots seamlessly.

COST EVALUATION

One of the primary tasks of the SAFE commission was to conduct a cost analysis of various voting systems. Aside from a question posed to each vendor related to what initial equipment costs would be, absolutely no consideration or analysis was provided related to ongoing costs. County election officials repeated abstract concerns related to ballot printing costs, and yet no discussion was held relating to ongoing maintenance and upkeep of BMDs. Likewise, no information was provided related to the costs of BMD supplies, such as thermal paper, and whether any of the systems required a proprietary source of supplies (and therefore higher ongoing costs) as opposed to open-market solutions. The Commission failed to meet its own limited mandate on this issue.

AUDITS

Whether the legislature decides in the end on an all-BMD system or a hand-marked paper ballot with accessible options for disabled voters, the ultimate safeguard to election integrity is mandatory post-election pre-certification audits. We are pleased that Commission’s majority report supports such audits. However, the Commission report does not go far enough. Significant progress has been made in both academic circles and government studies, and the broad consensus is that risk-limiting audits represent the best model for ensuring that the outcome of an election accurately reflects voters’ selections. As a minimum, the legislature should mandate that any audit must:

- Be conducted in public;

¹⁴ “It’s Time to Solve the Mystery of the 100,000 Missing Votes,” Jim Galloway, [The Atlanta Journal-Constitution](#), December 5, 2018.

¹⁵ SAFE Commission report, p. 14.

¹⁶ “Elections: Observations on Voting Equipment Use and Replacement,” p. 39.

- Consist of a manual examination of the paper records; and
- Examine a statistically significant number of paper ballots.¹⁷

Anything less than these requirements would be insufficient to provide confidence in the results of the election.

SUPPORT FOR RECOMMENDED CHANGES

We recognize and appreciate many of the additional changes in Georgia election law that have been outlined in the SAFE Commission report. We particularly support the following recommendations:

- Defining an official ballot. The only legally recognized ballot must consist of a paper record that is readable by a human without external assistance.
- Extending certification deadlines. Implementation of robust post-election audits will require extending county certification deadlines by at least one week. Such a move would also allow for extension of other deadlines, such as provisional cure periods.
- Recounts. The existence of a durable paper record will allow for hand-recounts in addition to recanvassing tabulation results. It is important to note that counties will need significant training and support in the conduct of both of these activities.
- Runoffs. Runoffs create additional burdens on counties and voters alike. The Commission report does not address the extraordinary difficulties that counties and voters face due to the differing treatment of state and federal races in a runoff. This difference means that registration rolls must be re-opened for federal race runoffs, while they remain closed for purposes of state runoffs. This differentiated treatment has led to voter confusion and enormous burdens on county election officials. The state legislature must eliminate this disparate treatment.
- Absentee ballots. We wholeheartedly support any changes to the absentee ballot process that would ensure that every qualified voter's ballot is counted. In addition to the recommendations contained in the Commission report, we would also recommend that rules governing UOCAVA ballots, counting absentee ballots that are postmarked by election day and received by three days after the election, be extended to all absentee ballots, as was applied for the December 2018 runoff election.
- Voter Assistance. We support these recommended changes.
- HAVA Verification. In addition to verification by county officials, we strongly encourage the incoming Secretary of State to study the issue of data transfer between the Department of Driver Services and voter registration records. The Democratic Party of Georgia's voter hotline documented scores of instances of voter registration records being inaccurate or having been changed without the voter's knowledge, frequently coinciding with the voter updating or renewing their driver's license. The adoption of automatic registration through the DDS was hugely beneficial to Georgia's voters, and should not be diminished. The system could use improvements in data accuracy, which would aid both individual voters and election administration.
- Advanced in-person voting. Georgia should be proud of its early voting opportunities. We concur with the recommendations that counties be provided with greater flexibility in identifying appropriate advance voting locations.

¹⁷ Securing the Vote: Protecting American Democracy, pp. 100-101.

One additional area of critical need that was not addressed by the SAFE Commission is the security of our voter registration database. Voter experiences and self-reporting during the 2018 General Election revealed that systemic problems exist in relation to the accuracy of our voter registration records. In addition, serious vulnerabilities in the registration system have been identified. In May 2018, the U.S. Senate Foreign Intelligence Committee released a report with recommendations for actions that states and local jurisdictions can undertake better to secure the critical infrastructure of our voter registration system. The Georgia General Assembly should undertake to ensure that these necessary steps are taken to protect our systems at both the state and the county level.

The [Senate Foreign Intelligence] Committee recommends State and Local officials prioritize the following:

- Institute two-factor authentication for state databases.
- Install monitoring sensors on state systems. One option is to further expand DHS's ALBERT network.
- Identify the weak points in the network, including any under-resourced localities, and prioritize assistance towards those entities.
- Update software in voter registration systems. Create backups, including paper copies, of state voter registration databases. Include voter registration database recovery in state continuity of operations plans.
- Consider a voter education program to ensure voters check registration well prior to an election.
- Undertake intensive security audits of state and local voter registration systems, ideally utilizing an outside entity.
- Perform risk assessments for any current or potential third-party vendors to ensure they are meeting the necessary cyber security standards in protecting their election systems.¹⁸

PROPOSED STANDARDS

In order to properly evaluate a system, a body must first establish standards by which different systems could be evaluated. This Commission did the opposite—instead of first setting standards, it requested information from vendors and based its evaluation on what was offered. This vendor-led, cart-before-the-horse approach allowed the Commission to come to a premature conclusion without providing the legislature with either a strong basis in facts and research or baseline standards for what Georgia is seeking in a voting system. This approach is not in the interest of the state or its voters.

A standards-based evaluation places the interest of Georgia voters and taxpayers first, by allowing lawmakers to determine priorities, and then places the onus on vendors to meet the

¹⁸ "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, *found at* <https://www.burr.senate.gov/press/releases/senate-intel-committee-releases-unclassified-1st-installment-in-russia-report-updated-recommendations-on-election-security>.

requirements set. Model voting system principles are widely available, but again, Commission members were never apprised of them.¹⁹

Voting system principles generally address such issues as security, functionality, privacy, auditability, usability, and accessibility. Although the Commission report purported to address many of these issues at the outset,²⁰ in fact some of the most critical issues were either ignored or disingenuously covered.

Security

The National Conference of State Legislatures (NCSL) defines security as follows:

A “secure” voting machine means one that cannot be tampered with or manipulated. Security begins with requiring that systems accurately record votes as cast. Although requirements vary from state to state, other aspects of security that may be addressed include:

- Physical security of the equipment and ballots: Procedures that ensure that additional votes cannot be cast after the polls have closed or tampered with at any stage of the process, and that there is an auditable “chain of custody.”
- Auditability: The capability of a machine to maintain an audit record that can be reviewed post-election.
- Internet connection: Ensuring a machine cannot be connected to the Internet or networked during the voting period to avoid the potential for hacking.²¹

The Commission’s own cybersecurity expert went to great lengths to explain cybersecurity concerns with different voting methods. He published three separate papers, and gave an address to the Commission at its second meeting. Despite his testimony, however, the Commission report framed Dr. Wenke’s points and concerns as isolated to him alone; by recommending a BMD system, the Commission essentially disregarded its own expert’s advice. We recommend that the legislature reinstate security as a primary, fundamental principle to which any new voting system must adhere.

In addition to cybersecurity concerns, physical security is likewise paramount. As the Commission report notes, robust chain-of-custody controls as well as physical security of all equipment and materials are of critical importance.

Functionality

¹⁹ See, e.g., “Voluntary Voting System Guidelines 2.0: Principles and Guidelines,” Election Assistance Commission (EAC), 2017, *found at* https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf; “Verified Voting Foundation: Principles for New Voting Systems,” Verified Voting, *found at* <https://www.verifiedvoting.org/voting-system-principles/>; and “Voting System Standards, Testing, and Certification,” National Conference of State Legislatures, Aug. 6, 2018; *found at* <http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx>.

²⁰ Draft SAFE Commission Report, p. 3.

²¹ National Conference of State Legislatures.

Again, the NCSL provides clear, concise guidelines with regard to how voting system standards should address functionality.²² The system must provide the highest confidence that it will:

- Accurately deliver the correct and appropriate ballot to every voter, reflecting every race and ballot question for which the voter has the right to vote;
- Correctly register and record all voters selections;
- Allow the voter to review, change, and verify their selections before casting their ballot;
- Notify the voter of over- and under-votes, and
- Permit voters to write-in candidates.

Verifiability should be assessed in real-world conditions.

Auditable

Verifiability is closely related to auditability. In order for the vote count itself to be auditable, the ballot records themselves must be truly verifiable. Vendors should be required to prove, via interactive demonstrations with legislators and staff, that their system produces a paper ballot trail that can be verified in real world conditions.²³

A voting system is auditable only if the system hardware and software cannot produce an undetectable change in the results. This means that the systems must produce records that can be examined and any changes that have been made to the programming made must leave a clear trail. Vendors should be required to demonstrate the systems they have in place to log and generate reports of any changes made to programming and other error messaging.²⁴

Privacy

Ballots, no matter what mode of voting is used, must not contain any mark or indication that would link an individual voter to their ballot choices or intent. Every vendor should be required to certify that whatever paper produced by their device, whether a ballot-on-demand paper ballot to be completed by hand or a ballot receipt produced by an electronic ballot marking device, contains no personally identifiable information related to the individual voter who made those selections.²⁵

Usability

Every portion of the voting system should be designed with the user in mind, whether the user of that portion of the system is a poll worker or a voter. This entails high functionality and ease of use of poll books; ballot-on-demand printers if they are part of the system; ballot design, whether on paper or electronically; and scanner technology.²⁶

Accessibility

The system must allow voters of all abilities the same right to access and cast their vote independently. This does not require that all voters use an identical system, but it does require

²² Id.

²³ See "Addendum to Security Requirements for Voting Systems," Wenke Lee (2018).

²⁴ VVSG 2.0, Principle 15 (2017).

²⁵ "Verified Voting Foundation: Principles for New Voting Systems," Verified Voting.

²⁶ VVSG 2.0, Principle 8 (2017); Securing the Vote: Protecting American Democracy, p. 79

that the state provide as equal an opportunity for independent voting as possible. Accessibility contemplates that:

- Voters of varying physical abilities have the same right to vote independently;
- Voters who have limited English literacy must have access, including in additional languages where required by law;
- The right to a secret ballot requires that no ballot paper be connected to an individual voter.

The SAFE Commission did not complete its mission to assess objectively different options for a new voting system in Georgia. Instead, it allowed vendors to drive the agenda and the discussion. The Georgia General Assembly has a second chance to get this right; we hope that they will look at all of the information and evidence available and establish standards that are in the best interest of Georgia's voters.