Security of Electronic Voting Systems in Collin County
Facts & Issues

Overview: focus and scope of study, overview of topic

In May 2016 the League of Women Voters of Collin County (LWV-CC) adopted a study titled "Security of Voting in Collin County." This study was prompted by the fact that the electronic voting systems used in Collin County were aging and perhaps vulnerable to tampering or other errors. The county's 1400 Diebold Accuvote touch-screen voting machines were purchased in 2003 with federal funds provided by the Help America Vote Act (HAVA) legislation. These machines served the county well, while being maintained by local information technology personnel. However, hardware parts are no longer available and existing machines have to be used for spare parts.

The Collin County Elections Department is recommending that new Direct Recording Electronic (DRE) voting machines be replaced soon, preferably by the May 2019 election. The county has already budgeted and set aside $10 million dollars for replacement of the voting machines. Following certification of voting machines by the state of Texas and the federal government, the Collin County Elections Office will issue requests for proposals (RFP's) in spring 2018 and will conduct tests of the proposed machines in summer 2018. Bruce Sherbet, Collin County Elections Administrator, anticipates that there may be three or four choices. The Collin County LWV wants to be part of the process of choosing our new voting machines.

The League of Women Voters has worked tirelessly to promote voting rights over the years. The League helped draft and pass the Help America Vote Act of 2002, including lobbying to fully fund it. The following is from the LWVUS program publication, Impact On Issues, 2016-18:

> *At the 2004 Convention, the League determined that in order to ensure integrity and voter confidence in elections, the LWVUS supports the implementation of voting systems and procedures that are secure, accurate, recountable and accessible. State and local Leagues may support a particular voting system appropriate to their area, but should evaluate them based on the "secure, accurate, recountable and accessible" criteria. Leagues should consult with the LWVUS before taking a stand on a specific type of voting system to ensure that the League speaks consistently.*
> *At Convention 2006, delegates further clarified this position with a resolution stating that the Citizens' Right to Vote be interpreted to affirm that the LWVUS supports only voting systems that are designed so that:*
> - *they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent; and*
> - *the voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent; and*

- *such verification takes place while the voter is still in the process of voting; and*
- *the paper ballot/record is used for audits and recounts; and*
- *the vote totals can be verified by an independent hand count of the paper ballot/record; and*
- *routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.*

At Convention 2010, delegates added the principle of transparency, so that the League would support voting systems that are secure, accurate, recountable, accessible and transparent.

In order that the League speaks with one voice at all levels, we are obligated to adhere to this position. We are free to study the attributes of various voting systems, but the League feels that in order to protect voter confidence and the integrity of elections, it is of great importance that there be a paper record that is verified by the voter and that can be used for audits and recounts. We may not adopt a position that is in conflict with these provisions.

Federal and state requirements, laws for voting systems

The United States Constitution outlines roles for both the state and federal governments in elections. States are given the authority to regulate the elections process itself. This includes the power to decide details of registration procedures, absentee voting requirements, establishment of polling places, and counting and certification of the vote. States are, in general, also responsible for covering the costs of elections. While election policy and regulations are decided at the state level, most states have decentralized the process so that details of election administration, including the choice of voting technologies, are done at the city or county levels.

As a result of the 2000 Presidential Election debacle, the federal government has exerted more direct authority over the administration of elections and mandated specific procedures for election reform. The **Help America Vote Act (HAVA)** of 2002 created new mandatory minimum standards for states to follow in election administration and also provided funding to help states meet the new standards, replace voting systems and improve election administration.

HAVA requires all states to provide a process for allowing voters to cast provisional ballots and to have at least one DRE machine per county to provide enhanced access to the voting process by people with disabilities. A provisional ballot allows voters whose voter registration status is in doubt to cast a vote pending review by the local election board.

Texas requires that its voting systems meet current federal standards as well as state requirements. The Texas Secretary of State accepts applications to examine and certify voting systems and appoints four people to examine the voting system. In addition, the Attorney General appoints two examiners. Each examiner inspects the voting system and submits a report to the Secretary of State. The Secretary of State conducts a public hearing to provide

interested persons an opportunity to express their views for or against the approval of the voting system. Following the public hearing, the Secretary of State prepares a written report stating why the voting system was approved or denied.

Currently there are three vendors and a total of seven voting machine systems that have been certified by the state. However, additional state examinations are in process to certify additional voting machine systems.

Counties in Texas may provide voting by paper ballot, optical scanner or DRE voting machine. However, DREs are required by the Texas Secretary of State for participation in countywide vote centers, which Collin County has supported since 2009. A DRE provides a screen display of ballot options and the voter makes a selection using buttons or by touching the screen. The selections are stored in removable memory components on the machine, which are then removed and used for tabulation of votes.

DREs increase the speed of vote counting and incorporate a number of technologies to assist persons with disabilities, allowing them to vote without forfeiting the anonymity of their votes. They can also provide immediate feedback to the voter detecting such possible problems as undervoting and overvoting (selecting too few or too many options, respectively, for a given ballot race). They remove the need to print large numbers of paper ballots, a significant cost, and eliminate the risk of running out of ballots. They can be programmed to provide ballots in multiple languages.

On the other hand, DREs are expensive and require training of personnel and voters. Moreover, there is a large amount of concern about how easily they can be tampered with. Some voters are also concerned that, although they can see a summary of their selections on the DRE before casting a final vote, they have no proof of how the vote is actually recorded in the DRE's memory.

Since Collin County plans to continue participation in the state's program for countywide vote centers, it is assumed that its electronic voting systems will be DREs or other equipment eligible for the program.

Systems currently used by Collin County

Voter Registration

Collin County elections personnel enter voter registration information into a county database using Votec software and authorized user accounts protected by user IDs and passwords. The database server is housed within the county data center, but there is no direct access between other county users and the database. Access to a web-based voter lookup feature is restricted to a service account with read-only access. The county's Information Technology (IT)

Department monitors and maintains the database, and follows standard IT practices to ensure that the data is secure and that software is updated with the latest published versions.

Data from the county database is uploaded daily to the state database, which by law is the official voter registration database. Although some smaller counties enter directly into the state database, Collin's personnel believe it is more secure to remain offline and perform daily batch updates. The Texas Secretary of State is required by law to participate in an interstate crosscheck program to prevent duplicate registration. If it is determined that a voter is registered more than once or in more than one state, the oldest registrations are canceled and the voter is notified.

EPollbooks

The county has 250 Lenovo T540 laptops available for use as "ePollbooks" at polling locations to check the voter registration status of persons who come in to vote. The laptops use on-board GOBI cards to establish a wireless internet connection through the county's mobile data services provider, much like a cell phone connection to the Internet. Once the direct communication is established, a virtual private network (VPN) is opened to provide a secure tunnel between the laptop and the server with the voter registration database. VoteSafe software performs real-time updates to the voter registration database when the voter is checked in at the polling place, and it alerts the election clerk if the system shows that the person has already voted. Each laptop has the entire voter registration database, so the lookup can be performed even if communications are down; updates would be made when communication is online again.

IT personnel monitor the connectivity of ePollbooks to server during elections. In order for an ePollbook to be compromised, someone would have to gain physical access to the machine in the polling site, which is unlikely since those systems are closely monitored and secured.

DRE Voting Machines

The county has approximately 1400 Diebold Accuvote touch screen voting machines purchased in 2003. Voting systems used in Texas must be federally and state certified prior to use. DRE units come pre-loaded with certified firmware. If an update to the firmware is needed, the county works with Dominion to perform the certified upgrades in accordance with state law requirements.

For each election, the county contracts with Dominion to configure the election database and create ballots. County elections personnel download the ballots to each DRE over a local area network (LAN). The program used on the DREs is thoroughly tested prior to being used in an election, with test ballots representing every ballot style and voting position on the ballot. The tests include uploading the test ballots to the tabulation server to verify that everything is

accumulating accurately. Initial proofing is performed by the elections department, and final approval is required from contracting entities and political parties (where applicable).

At the polling place, each voter is given a voter access card that identifies the correct ballot for the voter's precinct. Once the ballot is cast, the information on the voter access card is deleted before the card is ejected from the DRE unit, ensuring that the voter cannot use it to cast another ballot.

DREs provide bi-level verification of votes:

- Each DRE provides a **printed tape** with summary totals when the machine is closed at the end of early voting or at the end of Election Day. It is possible to print a "long report" also on the current AccuVote Touchscreen devices but election judges have been directed to only print the summary total reports. Printing a long report would produce a huge paper tape, but its information is preserved on the memory card from each machine.
- Each DRE has a **memory card** with individual ballot selections; this data is uploaded into a server for tabulation.

Procedures during Early Voting: At the end of each day of early voting, each DRE is sealed, numbered tamper-proof seal tapes are applied to the memory card slot, and the door that covers the memory card slot is checked the next morning before the start of voting to make sure nothing has been changed. At the end of the early voting period, the DREs are returned to the Elections Office, where the Ballot Board oversees the closing of each DRE and the tabulation of votes.

Counting Station personnel (tabulation supervisor, manager and judge) are responsible for the accumulation of vote totals. Memory cards containing ballot selections are removed from the DREs and uploaded to the tabulation server in the tabulation room, a standalone room that requires card access by authorized personnel only. Data on the tabulation server can't be compromised; logs are kept of all keystrokes on the server. A summary tape is also printed from each DRE showing total votes cast for each candidate.

Procedures on Election Day: Each DRE is opened in the morning by removing the numbered tamper-proof seal tapes and recording the numbers, and the door to the power button is resealed with a tape. At the end of the day the summary tape is printed, the memory cards and summary tapes are removed and all doors are resealed. The memory cards are used for final tabulation of votes at the Elections Office. The printed summary tapes and memory cards are stored in sealed bags.

Daily reports are completed by the election judge in early voting and on Election Day indicating the number of voters that signed in and are listed on the poll list, as well as the number of ballots that are cast on the voting units.

Reports generated from the server are posted on the county website and may be vulnerable to hacking, but the actual tabulation data is preserved. By state law, the data has to be stored for 22 months.

Optical Scanners and Paper Ballots

Optical scanners are used to count votes by mail. The Ballot Board verifies that signatures on application and ballot match, and then hand-feed ballots into optical scanner. If the ballot cannot be read by the scanner, it is "out stacked" to be reviewed manually by the Ballot Board. If the Ballot Board can resolve the problem, the revised ballot is fed into the scanner for tabulation.

Recounts

There have been no recounts in Collin County under the current Elections Administrator, Bruce Sherbet. However, he says that the data uploaded from the DRE memory cards can be printed in different formats, selected by office, precinct and other criteria to minimize the effort needed for a recount. The printout would provide a listing of individual votes cast, not just a summary. Those individual votes could then be hand-counted by two people, although this method may offer opportunities for human error.

DRE Replacements

Hardware parts are no longer available for the current DREs; existing machines have to be used for spare parts. Very few software updates are made, and those have to be certified by the state and federal governments. It is expected that new voting systems will provide better security, auditability and functionality.

The Collin County Elections Department recommends that the DREs and related equipment, including optical scanners, be replaced soon, preferably by the May 2019 elections. A review committee will be formed and public demonstrations will be conducted showing the available systems. Voter registration systems would be upgraded several years after the DREs, not at the same time, to minimize confusion.

Issues related to electronic voting systems

The LWVUS position supports voting systems that are secure, accurate, recountable, accessible and transparent. This section examines what is involved in ensuring these attributes.

Security of hardware, software, and processes:

A DEF CON cybersecurity conference is held annually in Las Vegas. At the 2017 conference, a "Voting Machine Village" was set up where attendees could try to hack a number of systems

and help catch vulnerabilities. The village had 30 machines, and all were hacked. However, some elections personnel say that with proper security processes in place, the threat to large elections is minimal, since the voting machines are not connected to the Internet and different machines are used in different counties. The elections most at risk might be local ones, although in a national election a hacker could target one or two key counties to swing a result.

The DEF CON experiment points out several issues in electronic voting systems security, including hardware, software and processes. Many of the problems with electronic voting systems are what you'd expect from any computer, especially one a decade or older. Most are running outdated operating systems, with no recent security patches. Many of them are susceptible to malware or a well-timed denial of service attack. If the machines don't work, or work slowly, that can prevent people from voting. Some voting machines have potentially vulnerable wireless components.

Most current voting systems use proprietary software based on Microsoft's operating system, which some people claim can be easily hacked. Instead, they propose the use of open-source software for which the original source code is made freely available and may be redistributed and modified. In the case of voting, open-source software systems would be overseen by public-private partnerships between counties and vendors. The Defense Department, NASA and the U.S. Air Force all use open-source systems. In open-source systems, anyone can see how they operate. Bugs can be spotted and fixed; however, hackers would also have access to the code. In closed-source systems, like Microsoft's, only the employees can see how they operate and fix bugs.

The location and interconnectivity of the voting machines are other factors in security. The systems most vulnerable to cyberattacks are large, centralized databases, where breaking into one part of the system can often give access to all of it. Connectivity to the Internet also presents a possible vulnerability to outside attack.

Polling place machines by necessity are situated in areas with public access, but they are generally standalone. Any attempt to hack them would involve accessing multiple machines in a public location, or possibly altering the machines' memory cards prior to insertion. The voting machines may have counters that can be cross-checked with other records to identify irregularities. They may also have devices to lock and/or seal them so that any attempts to access them are evident. Only physical ports and access points essential to voting operations are exposed.

Voter registration systems are more centralized, usually by county and/or state. Recent attempts to steal voter registration rolls raise the question of whether the lists of registered voters at polling stations could be manipulated. Deleting or altering registered voters could lead to additional processing time at the polls, resulting in long lines and frustration with the system. The communication protocol used by the computers polling stations to access the voter registration database presents another possible point of interference or hacking.

State law requires criminal background checks for all election officials, staff and temporary workers who are engaged in pre-election programming, testing and preparing of the voting system equipment for Early Voting and Election Day. This does not include poll workers (election judges and clerks) assigned to work election voting centers or precincts, but does include temporary workers hired to test, store, or service voting equipment. A person having a criminal record is not automatically disqualified from working with electronic voting equipment. However, the hiring entity should consider the nature of the crime(s) in determining whether to hire or assign voting system duties to an individual with a criminal record.

Election officials may develop processes to minimize any outside interference, such as:

- Limited access by authorized and trained personnel, using secure access methods such as user IDs and passwords
- Monitoring of systems and communications by qualified information technology personnel
- Storage of all equipment in secure locations
- Use of safety seals to detect unauthorized access to machines.

Accuracy of ballots cast, vote tabulations and reports

The accuracy of voting systems depends on the following:

- The ballot provided to each voter is correct for the voter's precinct.
- The voter can easily and clearly make desired selections on the machine.
- Ballot selections recorded in the machine accurately reflect each voter's selections.
- Each voter is allowed to cast only one ballot.
- Ballots cast are tabulated accurately.

There are several areas in which inadvertent errors or intentional malpractices can occur. A voter, after signing in, generally is given a card to insert into the electronic voting machine to determine which ballot selections are to be displayed based on the voter's precinct. If the wrong precinct is selected, the ballot will be incorrect. If the voter observes that the ballot selections offered are not the expected ones, he/she should be able to have the error corrected in order to cast a valid ballot.

Voters may make mistakes in choosing their selections, sometimes because the user interface is confusing or a "slip of the finger" in touching the screen selects the wrong option. A final review of selections before casting a final ballot allows the voter to correct such errors.

Sometimes there is confusion about casting the final ballot. In some DREs, the access card is ejected and the voter is instructed to return it to an election worker. However, it is possible for the voter to walk away from the machine before completing the final step. In that case, the vote is not recorded. Another type of voting machine requires the voter to press a big red button on a screen marked "Vote," and then the voter has to touch another button, "Confirm Vote." In one county in Kentucky that used these machines, election officials were convicted of

having the voters leave the booth as soon as they touched “Vote.” Then the election officials would review and sometimes change the votes before confirming the selection.

Even after reviewing selections on the screen and casting the final vote, on many machines the voter has no way of ensuring that his/her selections are accurately recorded in the machine. Independent paper audit trails have been cited as a method of allowing voters to verify that their vote was cast correctly and to provide a means to audit the electronic results. The two most commonly used forms include printing of a separate paper ballot that is then fed through a scanner into a locked ballot box, or printing of a paper record stored within the electronic voting machine that the voter can see but not modify, referred to as voter-verified paper audit trail (VVPAT). Printed paper records provide assurance to the voter that the vote has been accurately recorded, and they are available to use for audit or recount.

Some drawbacks to the paper audit trail include the expense of adding another component to the voting system that may be a point of failure (jams, running out of ink or paper) during the voting process, and the added time for the voter to verify the paper ballot. Voters are not required to check the accuracy of VVPAT records, may not take the time to do so, and may be confused by a different format on the paper record. VVPAT records are also subject to hacking, such as printing extra ballots when no one is looking (ballot stuffing) or invalidating a ballot. Paper ballots cannot be verified by many persons with disabilities.

According to Wikipedia, in the United States, 27 states require a paper audit trail by statute or regulation for all DRE voting machines used in public elections. Another 18 states do not require them but use them either statewide or in local jurisdictions. Five US states (including Texas) basically have no paper trail.

The votes that are recorded on each machine are then tabulated to calculate the vote totals. Tabulating machines may also be subject to hacking and require secure storage and monitoring. Unofficial voting results are often posted on websites on election night. It is possible that hackers could alter the unofficial reports. This would not alter the official ballot count, but could introduce mistrust about the numbers. By causing disruption, a hacker could cause people to lose confidence in the system.

Variety in types of reports available from data recorded on voting machines allows for multiple types of crosschecks for accuracy as well as efficiency in producing reports for analysis or even recounts.

Election officials may develop processes to minimize errors in recording and tabulating votes, such as:

- Testing of each ballot type and voting option after the ballot types are loaded
- Comparing manual voter sign-in records to votes recorded on machines
- Storing tabulation equipment in secure locations and monitoring their use

Recountability:

An election recount to re-tabulate the votes cast may be required or requested to determine the correctness of the initial count. Recounts may occur when the results are extremely close or some type of fraud or error is suspected. Recount methods generally depend on the type of voting system used and the records available. A Texas Secretary of State election advisory says that for a requested recount on a DRE, the candidate may request the recount be done electronically or manually.

With some electronic voting systems, the vote data collected from the voting machines can only be re-tabulated electronically. With DREs with VVPAT, or those that can print an image for each vote cast, the printed ballots can be hand counted. While electronic re-tabulations may not correct any errors originally introduced into the voting machines themselves, manual recounts can introduce "human errors." Multiple recounts by hand often produce a different result each time, especially when large numbers of votes are involved.

Accessibility:

The EAC's proposed Voluntary Voting System Guidelines state that a voting system should be accessible by "a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction."

Voting machines that provide clear instructions and are easy to navigate can minimize confusion and promote voter trust, as well as provide more accurate results. Training in use of machines before a voter goes to the polls may be helpful, either in person and/or online, especially when new machines are being introduced.

Persons with disabilities may not be able to mark, verify and cast their ballot using standard voting equipment or paper ballots. They may require special equipment or assistance from others. The Americans with Disabilities Act and other federal laws specify requirements, and voting systems must be able to meet those requirements.

Persons whose native language is not English may require language translations. The National Voting Rights Act of 1965 requires some ballots to be offered in multiple languages. Instructions for using the voting machine may also be required in multiple languages. State laws specify who may assist the voter with language translations in the polling place.

Transparency:

Transparency assures that the public can understand and verify the operations of the voting system throughout the entirety of the election, from selection of voting systems to the counting of votes.

When new voting machines are to be purchased, representatives of the public can provide helpful information about what features are important, whether machines are easy to use, and how confident the voter feels that the ballot is properly recorded. It's not just the use of taxpayer money that is at stake, but trust in the overall election process. Input from public representatives may slow down the process and lead to some disputes, but may in the long run prevent significant and expensive mistakes.

Testing of voting machines being prepared for elections is a tedious and painstaking task. For each election, Collin County elections personnel download the ballots to a DRE and perform tests using every ballot style and voting position on the ballot. Tabulation results are proofed by the elections department, and final approval is required from contracting entities (e.g., cities, school districts) and political parties (where applicable). Observation by the public during testing itself may promote trust in the system, but could also be a distraction, as well as provide an opportunity for outside tampering. Approval of the results by public representatives is less intrusive.

Tabulation of votes at the end of an election is generally performed in a secure location. In Collin County, the Ballot Board, representing the public, oversees the closing of each DRE and the tabulation of votes.

The election process at the polling places is public, held in public places with private citizens running them. Mistakes are made, and some workers and voters may try to cheat the system, but these numbers are generally small. Our election laws anticipate human error and cheating and guard against them at multiple levels. Local political parties appoint or nominate the election officials. The political parties work alongside and watch each other. Poll watchers can point out errors and irregularities to election officials and ask to have them corrected.

Efforts to rig the system would need to be systemic, with a predetermined outcome. To rig an election would require not just technological capabilities, but also the cooperation of partisan election officials and poll watchers.

Security of electronic voting systems

The right to vote freely and to have one's vote accurately counted requires more than reliable technology; it also involves the voter's confidence in the integrity of the entire system. The integrity of the right to vote is ensured by voting systems that are secure, accurate, recountable, accessible and transparent.

References

Federal and state requirements, laws for voting systems

- Election Assistance Commission (EAC) Help America Vote Act (HAVA) webpage, https://www.eac.gov/about/help-america-vote-act/
- EAC Voluntary Voting System Guidelines (VVSG 2.0) https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf
- Texas Secretary of State, Voting Systems webpage https://www.sos.state.tx.us/elections/laws/votingsystems.shtml

Systems currently used by Collin County

- League of Women Voters of Collin County Interview with Collin County Elections Administrator Bruce Sherbet and other Elections personnel, February 9, 2017
- League of Women Voters of Collin County Interview with Collin County Elections Administrator Bruce Sherbet, August 29, 2017

Issues related to electronic voting systems

- "Hackers breach dozens of voting machines brought to conference," Joe Uchill, 07/29/17, http://thehill.com/policy/cybersecurity/344488-hackers-break-into-voting-machines-in-minutes-at-hacking-competition
- "Rigging an election? It's not so easy, voting law expert says," NPR Fresh Air interview with Rick Hasen, founder of the Election Law Blog and professor of political science and law at the University of California, Irvine Law School, 10/25/16, http://www.npr.org/2016/10/25/499274789/rigging-an-election-its-not-so-easy-voting-law-expert-says
- "I'm a Republican election lawyer. Here's why the election can't be rigged," by Chris Ashby, Republican campaign finance and election lawyer, Vox Media, https://www.vox.com/the-big-idea/2016/10/19/13322270/pollwatchers-rigged-election-law-trump
- "Sowing doubt is seen as prime danger in hacking voting systems," by David E. Sanger and Charlie Savage, New York Times, Sept. 14, 2016, https://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html?rref=collection%2Fsectioncollection%2Fus&action=click&contentCollection=us&region=rank&module=package&version=highlights&contentPlacement=8&pgtype=sectionfront
- "America's electronic voting machines are scarily easy targets," by Brian Barrett, Wired, Aug. 2, 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/
- To protect voting, use open-source software," by R. James Woolsey (former director of the Central Intelligence Agency) and Brian J. Fox (creator of the Bash open-source software), New York Times, Aug. 3, 2017,

https://www.nytimes.com/2017/08/03/opinion/open-source-software-hacker-voting.html?ref=opinion

- Wikipedia, "Voter-verified paper audit trail," last edited Oct. 14, 2017, https://en.wikipedia.org/wiki/Voter-verified_paper_audit_trail
- "Voter Verified Paper Record Legislation," Verified Voting, https://www.verifiedvoting.org/resources/vvpr-legislation/
- Wikipedia, "Election recount," last edited Oct. 14, 2017, https://en.wikipedia.org/wiki/Election_recount
- Wikipedia, "DRE voting machine," last edited Sept. 23, 2017, https://en.wikipedia.org/wiki/DRE_voting_machine
- "Conducting Criminal Background Check pertaining to House Bill 2524," Texas Secretary of State Election Advisory No. 2012-02, https://www.sos.state.tx.us/elections/laws/advisory2012-02.shtml