Tales from the Trenches: Case Studies in Election Cybersecurity Preparedness in Texas

Elizabeth Kasongo[1,3], Matthew Bernhard[2], and Chris Bronk[1]

[1]University of Houston, [2]VotingWorks, [3]Louisiana Workers' Compensation Corporation

Abstract. Events surrounding the 2016 election violently shook the U.S. elections environment. Since then, numerous policy changes have been implemented. Despite this, the 2020 election was still one of the most contentious elections in U.S. history, up to and including historic-levels of violence and unrest. We conducted post-mortem interviews with three election officials at the county level in Texas to get a better idea about what went well, what when poorly, and what must be addressed going forward. How well did the policy changes post-2016 bolster our confidence in elections in 2020? The answer is quite a lot, but not enough to accommodate new issues like the COVID-19 pandemic and unforeseen levels of domestically-generated misinformation, which overshadowed policy successes in securing systems from outside manipulation by cyberattack.

1 Introduction

The 2016 U.S. presidential election witnessed overt attempts by foreign powers to influence the outcome [23]. Multiple elections jurisdictions across the U.S. experienced attempts to infiltrate the infrastructure they use to conduct elections, with infiltration succeeding in at least two states [9]. In the wake of these attacks, significant effort was made to shore up the defenses of elections in the United States, including significantly more funding for elections [25], the establishment of the Cybersecurity and Infrastructure Security Agency (CISA), and major emphasis on information sharing bodies like the Information Sharing and Analysis Centers and Organizations [11]. Numerous social media companies also significantly revamped efforts to combat misinformation that was widespread during the 2016 elections.

These efforts were largely successful, with the U.S. elections community concluding that the 2020 presidential election was "the most secure in American history" [13]. Despite this assessment and the tremendous amount of money and effort poured into election infrastructure, the U.S. witnessed something extraordinarily rare after the 2020 election: political violence. On January 6th, hundreds of people stormed the U.S. Capitol building, injuring the security force attempting to protect the building and killing one officer [4]. Calls of violence have run rampant after the election, and even elected officials expressed serious skepticism, up to and including voting against certifying the election results [29].

In this paper, we attempt to shed light on how these two seemingly disparate things can both be true at the same time: elections in the U.S. are more secure

than ever before, and yet discontent with the electoral system and concerns about its security are at an all time high. We argue that many of the policy changes made post-2016 did have a significant impact on the robustness of the electoral process, as shown by the deft response to an unforeseen and formidable challenge: the COVID-19 pandemic. Much of the policy changes made in the wake of 2016 empowered information sharing and the acquisition of better election equipment, which made states' efforts to transition to processes that limit the spread of coronavirus significantly easier. Whereas elections in years past had struggled to respond to the ever changing landscape, the increased resources and awareness allowed jurisdictions to respond rapidly.

However, these rapid responses also created a new problem: the spread of misinformation. We conducted interviews with three election officials in Texas, a state that saw dramatic changes to its election policies in response to COVID-19, including extended early voting periods and modified rules around absentee voting [30]. All three interviewees indicated that the election itself went smoother than anticipated, but that misinformation proved to be a much more difficult issue to contend with. In an environment where election logistics were changing rapidly, and one where the spread of misinformation had already proven to be an effective attack vector, voters were bombarded with constantly changing and inconsistent information about when, where and how to vote. Worse, voters were also subject to conspiracy theories heralded at the highest level of government about the insecurity of voting systems and the illegitimacy of the election results [3].

Our interviews with elections officials helped us to better understand that worked and what did not work in Texas in 2020. We find that the additional resources and communications greatly bolstered the security and efficacy of elections. However, our interviewees also expressed great concern over the rise of misinformation, suggesting that while efforts to improve elections in Texas and the U.S. at large have had some success, significantly more work is needed.

The rest of this paper is structured as follows: in Section 2 we give a brief overview of elections in the United States, as well as the key policies that constrain them. In Section 3, we describe how and why we chose to interview election officials to shed light on the state of elections in the U.S.. We present case studies based on our interviews in Section 4, Section 5, and Section 6. Finally, we conclude in Section 7, synthesizing the knowledge our research has revealed and providing some recommendations for policy changes and future lines of research.

2 Elections in the United States

Elections in the United States are a complex system of multiple government entities with different degrees of jurisdiction, a small number of vendors, and a onerous regulatory regime. For brevity we choose to elide much of the complexity, and will try to provide just enough context to support the remainder of the paper.

2.1 Whose election is it anyway?

As the United States is a republic of states, its constitution delegates the vast majority of election responsibilities to the states, who in turn may delegate responsibilities down to local counties or townships. The exact degree of delegation varies widely between states; for example the states of Hawaii and Georgia largely run elections at a state level, handling most of the logistics and administration centrally while delegating the running of polling locations to counties. In contrast, states like Michigan and Wisconsin delegate almost all tasks to the local township level. Therefore, where responsibility for election security lies varies widely with each state.

In Texas, the state where our interviews were conducted, counties perform most of the election procedures. The state performs some regulatory tasks like deciding which type of voting equipment counties may purchase, distributes funding from the state and federal governments, and enforces policies about when and how elections may be conducted. However, county election officials ultimately have the power over what type of voting equipment to purchase (provided it is approved by the state) and therefore how voters are allowed to cast their ballots. Texas has a variety of voting technology, ranging from all-electronic DRE systems to hand-marked, hand-counted paper ballots. Most counties use a combination of voting technologies to accommodate absentee voting, voters with disabilities, and other considerations like the need for ballots in multiple languages.

County officials must also maintain significant information technology infrastructure, including: websites and social media accounts on which election information is distributed; email servers; and the technology required to maintain and program voting equipment, including voter information, ballot preparation and tabulation, and results reporting.

2.2 Help America Vote Act

Most of the requirements surrounding voting systems trace their lineage to the Help America Vote Act of 2002 (HAVA). HAVA was passed in response to the 2000 presidential election, in which a close contest ultimately came down to ballots cast on out-dated and poorly usable voting equipment in the state of Florida [16]. HAVA provided $2 billion to states to upgrade their outdated voting equipment. HAVA also created several new regulations about voting equipment, including the Voluntary Voting System Guidelines (VVSG), requirements against which voting equipment can be certified. The VVSG includes performance and correctness requirements, as well as requirements that voting systems accommodate voters with disabilities.

HAVA is widely regarded as having brought direct-recording electronic voting machines (DREs) into popular use, as they were some of the only market-ready equipment at the time that could meet VVSG requirements for accessibility. In the years since HAVA's passing, DREs have fallen out of favor due to their insecurity, and been replaced with a wide array of technology, including hand-marked, optically scanned paper ballots and ballot marking devices [8]. Because

certification to VVSG standards is expensive and time-intensive, voting technology tends to lag behind modern technology standard. Until the passage of VVSG 2.0 this year (an update to the standard), the security of voting technology was an after thought as it was not required for certification.

HAVA is also the mechanism through which federal funding is made available for elections. In 2019 and 2020 two disbursements of HAVA money were made, with the first designed to improve election security [25] and the second designed to bolster states' responses to the COVID-19 pandemic as part of the CARES Act [14].

2.3 Elections in Texas

Texas is a state in the southern region of the United States, among one of the largest states with a population of approximately 29,145,505 based on 2020 estimates [34]. Texas has approximately 16,955,519 registered voters as of November 2020 and 8,745 precincts as of November 2018 [35].

The state does not have stringent requirements on type of voting equipment deployed to polling locations, however it does require that systems be certified by the U.S. Elections Assistance Commission. In practice, this means that systems in Texas are certified to the first version of the VVSG, which dates to 2005. This version of the VVSG contains little in terms of security requirements from voting systems. In addition to EAC certification, Texas also retains independent certification, such that a voting system may not be certified in Texas even if it is EAC certified.

The outdated standards and otherwise somewhat laissez faire environment means that Texas is one of the most diverse states in terms of voting equipment. Systems in Texas range from hand-marked, hand counted paper ballots to ballot-marking devices to DREs that have no paper record at all [35]. Texas also supports early voting, where voters can vote in a polling location several weeks before the official electoin day. Texas additionally supports absentee voting, however voters must qualify to vote absentee via a number of conditions, like disability, military status, or out-of-state residence at the time of the election.

2.4 The 2016 election and its aftermath

The 2016 election was one of the most contentious elections in recent memory. Misinformation and hacking campaigns were carried out by numerous foreign actors to attempt to sway the election, the most prominent being Russia [23]. Election officials around the country were often caught off guard and unable to respond to these attacks due to lack of resources, training, and communication (a fact which all three of our interviewees confirmed).

In response to the shortcomings of the 2016 election, the federal government designated elections as critical infrastructure, which provided additional support from the federal government to elections infrastructure, and established the Cybersecurity and Infrastructure Security Agency (CISA), tasked with aiding sectors like elections in improving their robustness to cyber attack. Additional

emphasis was placed on Information Sharing and Analysis Centers(ISACs) with the establishment of the EI-ISAC, channels through which information like critical security vulnerabilities and incidences could be disseminated to local elections officials [11].

In 2019 additional HAVA money was disbursed to allow jurisdictions to upgrade their aging voting equipment. All three of the election officials we spoke to had recently upgraded at least some of their voting equipment in part due to this additional funding.

In addition to the federal push to improve election security, the state of Texas passed two bills to improve the state's ability to repond to cyber attacks. Texas passed House Bill 8, the Texas Cybersecurity Act, in 2017, which "provides specific measures to protect sensitive and confidential data and maintain cyberattack readiness." The bill was passed partially in response to the state's being targeted in 2016 [21], but also due to the widespread increase in cyber attacks against the state in recent years [6]. Texas House Bill 9, the Texas Cybercrime Act, was passed as a companion bill that "updates the Texas Penal Code to recognize several new types of cybercrime and their punishments." These laws expand officials' roles to protect essential data for which they are responsible.

2.5 The COVID-19 pandemic

In response to the COVID-19 pandemic, most states rapidly pivoted their election infrastructure to de-emphasize in-person voting, believed to carry and increased risk of transmitting the disease. States greatly expanded voting by mail, extended voting hours, and procured extra equipment to be used in polling locations to limit the spread. An additional $400 million was disbursed to states via HAVA [14]. In total, more voters voted through non-traditional means in 2020 than ever before [28].

However, while some states like Michigan, Arizona, and Wisconsin could pivot to sending out ballots by mail, some policies proved inflexible. The absentee ballot counting period in these states does not ordinarily start until election day, as historically most voters vote in-person and the proportion of vote-by-mail ballots is relatively small. Amidst a tsunami of mail in voting, however, these counting rules led to significant delays in results reporting on election night. These delays were fodder for misinformation campaigns, and helped fed into the narrative that the election results were illegitimate [12], a narrative that was picked up by elected officials in Texas and elsewhere [19].

3 Examining preparedness

In order to delve into the effectiveness of measures taken post-2016, as well as to assess how an election could be "the most secure in American history" while simultaneously resulting in political violence, we set out to interview election officials who were responsible for running the 2020 election. We solicited interviews with several, and conducted interviews with three election officials over seeing

County	Registered Voters	Type of in-person voting system	2020 Elections budget (USD)	Budget per registered voter
Harris	2,480,522	BMD	$12,362,000	$4.98
Bexar	1,189,373	BMD+DRE	$4,278,082	$3.60
Cameron	218,910	HMPB+BMD	$1,498,560	$6.85

Table 1. Case Study Counties in Texas with Details—Summary data for the three counties where we interviewed election officials. Harris is the largest county in Texas and second largest county in the United States. Bexar County comprises about half of Harris's population, and Cameron County one tenth. All three counties spend similar amount of money per voter on elections.

medium- and large-sized counties in the state of Texas. Texas was chosen in part due to proximity to the researchers as well as it represents a good mix of election policies, voting equipment, and demographics in comparison to the United States as a whole [34, 35]. Together, the election officials we interviewed oversee elections for 23% of voters in Texas [35].

We interviewed officials from Bexar, Cameron, and Harris counties (who chose to remain anonymous) with the hope of understanding how secure their voting systems are and whether they have the necessary resources to provide the best security for the voting machines. A summary of information about the counties we interviewed can be seen in Table 1.

The interviews we conducted were semi-structured, with a predetermined set of questions to prompt our interviewees, shown in Appendix A. We focused on four main areas with each official: their voting system, election preparation procedures, experiences in 2020, and an overall takeaway about the security of their election system. All interviewees signed a consent form and clarified whether they wished to remain anonymous.

4 Case Study: Bexar County

With San Antonio as the county seat, Bexar County is the fourth most populated county in Texas and the 16th most populated in the United States. The county's election department is led by Elections Administrator Jacquelyn F. Callanen, a non-partisan candidate appointed by the election commission, including county judge, clerk, and more. Like other counties, "[t]he Bexar County Elections Department is responsible for voter registration activities and election operations throughout Bexar County."

We interviewed a Bexar County official who answered questions regarding election security and voting systems used in the County. During the interview with the County official, we asked questions about the voting processes and procedures. Below we provide a summary of the information provided to us by the official, along with quotes where relevant.

Voting equipment Prior to the 2020 election, Bexar County used Direct-Recording Electronic (DRE) as its voting system for 17 years. In November 2019, Bexar County finally decided to upgrade its voting system to what they now call blended or hybrid system purchased from ES&S. While a "hybrid" system has colloquially become known as a ballot marking and tabulation all-in-one device [37], Bexar County's system is a separate BMD and scanner for most voters. Texas also supports "curbside" voting, where voters who cannot enter a polling place due to a disability vote on a machine brought to the vehicle that transported them to the polling location. Bexar County's new system includes paperless DREs for curbside voters [35].

Election preparation Bexar County's election preparation process differs from the other counties because it services the three military bases. Voters who are in the military or overseas fall under a different set of regulations than most voters: the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [32]. Forty-five days before the election, UOCAVA requires thatthe County elections department to send all the military ballots to the bases, in addition to sending absentee ballots to UOCAVA voters overseas. Failure to do so on time results in the county covering the ballots' delivery and returning costs.

Because of this early deadline, the interviewee indicated that preparations for the election begin six months before election day. Early preparation includes equipment testing and inspection of other systems like voter registration. During this period, the election administrator holds weekly meetings with staff to brief on all critical functions that must be completed before the election.

Experiences in 2020 Despite all of the changes incurred by rolling out a new voting system, dealing with the COVID-19 pandemic, and rampant misinformation campaigns led by foreign adversaries [22], the official we spoke with in Bexar County felt that the election overall went smoothly:

> I am unbelievably proud of my team and how well we worked in November... CISA made us essential workers which means that we spent over 90 hours in the office together... [we witnessed] the most voters, mail-in ballots, the governor extended early voting which helped. The County paid for all election officials to test for COVID-19... spent about half-million dollars to ensure everyone is protected.

The official alleged that in 2016, the Texas Secretary of State's (SOS) system was hacked. However, the then-Secretary of State denied that the state was a victim of the Russian hacks, asking the DHS to make corrections of the list they published [21]. Nevertheless, Bexar county opted to develop new protocols to provide better defense against cyberattacks.

> We have written protocols to protect ourselves in case the SOS gets hacked. We now have a complete shadow election set up that is moved

> offsite and double locked. Should something happen, we will still be able to get elections results. Prior to 2016, we never thought of this. The climate changed a little bit.

The interviewee also indicated that better communication was a boon to preparing for this election, citing both CISA's role in the 2020 election as well as Texas's emergency operations center, statingt that they "[w]ork hand-in-hand with them and see if we can remediate anything from the back-end."

Despite these changes, Bexar County experienced an unexpected problem during the 2020 election that left voters confused and contributed to misinformation spreading across the jurisdiction. In contrast with their old DRE system the new system sees voters handling paper ballots and placing them in the tabulator; however, no one was aware that those boxes could only hold 2,000 ballots. Election workers at the precincts were under the assumption that the tabulator was jammed when the tabulators filled up and they could not push through ballots. Voters began thinking that the tabulators were not working, and misinformation circulated rapidly within the county, to the extent that voters started leaving the polling locations without having voted. The official we interviewed explained that "everybody focused on hardware and software. No one informed us of the number of ballots held by the tabulator."

As the administrator only had five election technology specialists working to cover 45 polling locations, they had to bring extra technicians from other departments to change the tabulators. Fortunately this issue was mitigated slightly be the changes to early voting rules to accommodated the pandemic, as during early voting voters can go to any polling location. This spread out the load on individual locations and resulted in tabulators filling up less frequently.

Takeaways Overall, the official we spoke with agreed that Bexar County is well-equipped to defend the voting systems and voter information from cyberattacks. The official cited their newly adopted policies, annual voting systems inspection by the vendor, the ability to tabulate absentee ballots earlier than election day, the use of electronic pollbooks; as well as in-house databases, VPNs, and password policies, and that "the voting system is encrypted" with an "encryption method signed off by [the] federal government and State of Texas."[1]

5 Case Study: Cameron County

Cameron County is located in the southernmost part of Texas, bordered to the south by Mexico and to the east by the Gulf of Mexico, with Brownsville as the county seat. Cameron County has approximately 218,910 registered voters in approximately 102 precincts.

[1] As ES&S has never submitted their systems for independent review, and the standards used to certify the system used in Bexar county only requires encryption for electronic transmission [31], we could not verify these claims about encryption.

Voting equipment Cameron County uses hand-marked paper ballots with ballot marking devices for accessibility, and an optical scanner for tabulation. They follow a precinct count voting system where the ballots are tabulated at the polling location [35]. Our interviewee indicated that the county uses two backup methods for voting counts and results to avoid data loss, including utilizing a USB drive and an internal record. The presiding judge brings the copy of the counts to the central location, and if an issue arises, an individual is sent to collect a copy of the USB drive and machines.

Election preparation Expounding on procedures around the voting equipment, the official explained that there is ongoing security surveillance of the County IT system. When setting up a machine for the next election, the machine's state is verified to ensure that nothing has changed while the machine was in storage. Then, machines are programmed with data for the upcoming election over an Internet-connected virtual private network, and security patches are installed. (This manner of connection adds risk of compromise due to Internet exposure.) A week before the start of early voting, the public is invited to view logic and accuracy testing, where machines are tested to ensure the election programming is correct.

For other election-related procedures, like communication, transferring voter data, and aggregating tabulation results, the interviewee reported the use of VPNs, FTP, and software access controls for all software that is used. Additionally, the official indicated that the elections warehouse was physically secured. While they reported not using encryption on their office systems, they encrypt data transferred to locations with no additional security layer.

Experiences in 2020 After 2016, the interviewee reported that there were significant concerns regarding the security of Cameron County elections and voting systems, including a past data breach. However, they noted significant improvements to their security posture. Funding from the state and grant money from two outside entities allowed for better security of their voting equipment. They also noted a precipitous increase in cybersecurity training and awareness, and established processes for handling phishing attacks and other suspicious incidences. The interviewee also cited better communication between federal, state, and local officials, " with the [cybersecurity] training, we all started speaking the same language and understand each other."

Takeaways When asked how prepared Cameron County was to face cyber threats, the official responded by stating, "[e]very election offers its challenges. COVID-19 was a challenge for us, and the machines did not have any problems. Using the paper-based system, COVID did not have as much impact." Overall, the interviewee expressed confidence that Cameron County did provide adequate security for its voting systems, but identified misinformation as a major threat:

> [We will] try our best to make sure that information [that we share with the public] is legitimate. After 2020, misinformation is becoming a danger to our elections and we need to provide additional training [to the public and staff] to recognize it. The awareness of the threat has increased since 2016. The more information we have, the better we can protect ourselves and our democracy.

6 Case Study: Harris County

Harris County is the largest county in Texas, with an estimated population of over 4,713,325. The County's election department is under the leadership of County Judge Lina Hidalgo and elections administrator Isabel Longoria. According to VerifiedVoting, Harris County had over 2,480,522 registered voters as of November 2020, with an estimate of 1,012 precincts [35].

We interviewed Michael Winn, the Harris County Chief Deputy Administrator, who has over 25 years of experience working in the government. Mr.Winn agreed to be identified in our paper. He has worked in Bexar, Travis, and Harris Counties in the elections department and is on the Election Assistance Commission Board of Advisors. He was also one of the election officials who contributed to the development of STAR-Vote, an end-to-end cryptographic voting system [5].

Voting equipment Harris County has used DREs as their primary voting system since 2001, including during the 2020 general election, although they are currently transitioning to an all-BMD system for in-person voters.

Election preparation When preparing for elections, Mr.Winn identified three preparation windows, which include 45, 60, and 90 days before elections. During these periods, they conduct hash code testing to verify whether the code matches a hash code that was previously taken. If they do not, they choose to replace the system due to the possibility of the system being tampered with. They also perform the logic and accuracy testing to ensure that machines are programmed correctly for the upcoming election.

Forty-five days before the elections is known as the "lockdown period", where the system is air-gapped. During the preparation period, the county involves its partners to check that their information such as addresses, contact and more is correct, including schools, political parties, and polling places. Per Mr.Winn, this process, known as entity proofing, is a vital means of ensuring the correctness of public information.

During the interview, we asked Mr.Winn how the County deals with equipment security. He explained that "if there are updates [to the voting system software], we do communicate with vendors... we do get the updates and when completed, there is a file, a record that shows that there has been an update and it outlines the details of it including dates and times. Record is sent to the state [the Secretary of State], and they have a version of the last update." He reported

that the county uses encryption to protect their systems and voter information. To backup votes or results, Harris County performs audits during tabulation; with the old DRE system, this involved printing periodic results tapes from the machines to compare with other data collected during the election.

According to Mr. Winn, Harris County has a team of information technology (IT) specialists who provide the election officials updated on their voting equipment status and any critical information they need to know daily. The county also ensures that education and training are provided for every employee and encourages them to become certified in election security. They also have a program such as the automatic shutdown of programs when the computers experience inactivity, mitigating insider threat.

Experiences in 2020 When we asked Mr. Winn how the 2020 presidential elections differed from 2016, he responded, saying that "there was more communication between CISA, DHS, FBI. Continuation efforts to make sure that county officials become a part of the decision-making of elections. The government was keeping information to themselves [in 2016]; part was to avoid vulnerability. In 2020, there was the inclusion of all officials."

Takeaways As Harris County is Texas's largest county, one might assume that they have all the necessary tools and are well equipped to secure elections and electoral infrastructure. However, when posed with the question of whether Harris County is well equipped to protect the voting systems and voter information from cyberattacks, Mr.Winn's response was no different from the other officials we interviewed: "nothing is guaranteed, our county does a good job of making sure that we stay current and make sure we have the best system in place. We just purchased a new voting system that will be used for the first time in May 2021."

7 Conclusion

We set out to understand two incongruous facts: the 2020 election overall appears to have run smoothly and largely without incident, and yet it has led to some of the most tumultuous political discourse in recent memory in the U.S. We provided some context for elections in the United States, and then performed interviews with three election officials in the state of Texas to get a better picture on the ground. All three of our interviewees echoed that the election went well, and all three also indicated that the elections could have gone better from a security stand point.

What went well All three interviewees noted that there was significantly better communication at all levels of government about cyberthreats. Even in the presence of active threats [22], officials were able to move quickly to shore up defenses and quash any issues that might affect voters. Significant policy changes

and an increase in resourcing at all levels of government post-2016 also enabled a much more nimble response to the COVID-19 pandemic. Voters in Texas voted in unprecedented numbers in 2020, including a nearly 10-point increase in turnout and record high numbers of absentee and early voting [10, 36].

Improved communication at all levels of government played a key role in making the 2020 elections some of the smoothest and most secure in history, according to our interviewees. Federal initiatives like the founding of CISA and the EI-ISAC opened channels of communication between elections officials and intelligence officials that was pinpointed as a major problem in 2016 [17].

What went poorly Despite the major improvements, the 2020 election was not without its flaws. Issues ranging from delays in results reporting [15] to rampant misinformation campaigns still hindered public confidence in the election outcome [24]. Misinformation about results reporting flourished even despite serious efforts to communicate about the expected delays [26]. One of our interviewees saw firsthand how a run-of-the-mill problem in an election, like their scanners filling up with ballots, could lead to misinformation that ultimately led people to walk away from voting. All three of our interviewees noted that misinformation is one of the tallest hurdles to U.S. elections moving forward.

Unfortunately, misinformation is already having a significant impact on elections in Texas and the U.S. at large. The Texas Senate recently proposed more restrictive voting laws that would dramatically change the voting landscape in Texas [33], largely in response to misinformation that has spread after the election [2]. Many other states are considering similar laws, as well as withstanding partisan efforts to attempt to overturn the 2020 election outcome [1].

Takeaways The U.S. has made significant strides to improve its election security post-2016. Improved training and resources to election officials, improved communication between government entities, and improved processes all made 2020 a much smoother election than 2016. Practices long heralded by the election security community, like risk-limiting audits [18] and paper ballots [27], are seeing widespread adoption [20].

Despite these successes, misinformation continue to run wild, spurring legislative action [33], partisan campaigns to undermine elections [1], and leading to violence [4]. Research in combating misinformation is in its relative infancy, but our key takeaway from our discussions with election officials is that it is the single most important election security issue right now. Prior election security efforts have focused on providing voters with evidence, ranging from end-to-end encrypted voting systems to plain paper ballots and transparent counting [7]. However, it appears that merely *providing* this evidence is not enough: we need to be proactive in *using* it to convince voters that the election outcomes are secure.

Acknowledgements We would like to thank the election officials who agreed to speak with us. Their courage and insights helped us paint a clearer picture of the landscape of elections in the United States.

References

1. Anglen, R., Randazzo, R.: Arizona Senate considers expanding audit of Maricopa County ballots to all races. https://www.azcentral.com/story/news/local/arizona-investigations/2021/05/14/arizona-senate-considers-expanding-audit-maricopa-county-ballots-all-races/5100735001/ (2021)
2. Astor, M.: A Perpetual Motion Machine': How Disinformation Drives Voting Laws. https://www.nytimes.com/2021/05/13/us/politics/disinformation-voting-laws.html (2021)
3. Barrett, T., Raju, M., Foran, C.: Top Republicans defend Trump on baseless voter fraud claims as concerns grow in the ranks. https://www.cnn.com/2020/11/05/politics/election-2020-congressional-republicans-trump-election-fraud/index.html (2020)
4. Barry, D., McIntire, M., Rosenberg, M.: 'Our President Wants Us Here': The Mob That Stormed the Capitol. New York Times (2021), accessed from https://www.nytimes.com/2021/01/09/us/capitol-rioters.html
5. Bell, S., Benaloh, J., Byrne, M.D., DeBeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S., Winn, M.: STAR-Vote: A secure, transparent, auditable, and reliable voting system. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) (2013)
6. Benton, Jackie: Cyberdefense for Texas State Government. https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php (2019)
7. Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y., Stark, P.B., Teague, V., Vora, P.L., Wallach, D.S.: Public evidence from secret ballots. In: International Joint Conference on Electronic Voting. pp. 84–109. Springer (2017)
8. Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K., Halderman, J.A.: Can voters detect malicious manipulation of ballot marking devices? In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 679–694. IEEE (2020)
9. Bruer, W., Perez, E.: Officials: Hackers breach election systems in illinois, arizona. https://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems (2016)
10. Cai, M.: At least 9.7 million Texans — 57% of registered voters — voted early. https://apps.texastribune.org/features/2020/texas-early-voting-numbers/ (2020)
11. Center for Internet Security: Elections infrastructure information sharing and communication (ei-isac). https://www.cisecurity.org/ei-isac/ (2021)
12. Chen, E., Chang, H., Rao, A., Lerman, K., Cowan, G., Ferrara, E.: COVID-19 misinformation and the 2020 US presidential election. The Harvard Kennedy School Misinformation Review (2021)
13. Cybersecurity and Infrastructure Security Agency: Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election (2020)
14. Election Assistance Commission: 2020 CARES Act Grants . https://www.eac.gov/payments-and-grants/2020-cares-act-grants (2020)
15. Henley, J., Sullivan, H., McCarthy, T.: When will we know the US election result – and why the delay? https://www.theguardian.com/us-news/2020/nov/06/when-will-we-know-the-us-election-result-and-why-the-delay (2020)
16. Jones, D., Simons, B.: Broken ballots: Will your vote count? CSLI Publications Stanford (2012)

17. Kamarck, E.: The federal-state disconnect in securing the 2016 election and how not to repeat it. https://www.brookings.edu/blog/fixgov/2019/08/23/the-federal-state-disconnect-in-securing-the-2016-election-and-how-not-to-repeat-it/ (2019)
18. Lindeman, M., Stark, P.B.: A gentle introduction to risk-limiting audits. IEEE Security & Privacy **10**(5), 42–49 (2012)
19. Livingston, A., Mulcahy, S.: As states count votes, some of Texas' most prominent Republican politicians are spreading misinformation about the election. https://www.texastribune.org/2020/11/06/texas-republicans-trump-results/ (2020)
20. McCadney, A., Howard, E., Norden, L.: Voting machine security: Where we stand six months before the new hampshire primary. Brennan Center for Justice. Retrieved from https://www. brennancenter. org/our-work/analysisopinion/voting-machine-security-where-we-stand-six-months-new-hampshire-primary (2019)
21. Najmabadi, S.: Texas denies state was target of election-related hacking by Russia. https://www.texastribune.org/2017/09/29/texas-denies-it-was-target-election-related-hacking/ (2017)
22. National Intelligence Council: Foreign Threats to the 2020 US Federal Elections. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf (2021)
23. Office of the Director of National Intelligence: Assessing Russian Activities and Intentions in Recent US Election. https://www.dni.gov/files/documents/ICA_2017_01.pdf (2017)
24. Ognyanova, K., Lazer, D., Robertson, R.E., Wilson, C.: Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. Harvard Kennedy School Misinformation Review (2020)
25. Parks, M.: Congress Allocates $425 Million For Election Security In New Legislation (2019)
26. Riccardi, N.: AP Explains: The election result may be delayed. That's OK. https://apnews.com/article/election-2020-biden-trump-delayed-result-d9208787554db4c4575579f6b75a7cde (2020)
27. Rivest, R.: On the notion of 'software independence' in voting systems. Phil. Trans. R. Soc. A **366**(1881), 3759–3767 (October 2008)
28. Scherer, Z.: Majority of Voters Used Nontraditional Methods to Cast Ballots in 2020. https://www.census.gov/library/stories/2021/04/what-methods-did-people-use-to-vote-in-2020-election.html (2021)
29. Sprunt, B.: Here are the republicans who objected to the electoral college count. https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/07/954380156/here-are-the-republicans-who-objected-to-the-electoral-college-count (2021)
30. of State, T.S.: Covid-19 resources for election officials. https://www.sos.state.tx.us/elections/covid/index.shtml (2020)
31. United States Election Assistance Commission: The Voluntary Voting System Guidelines 1.0. https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines (2005), accessed both volumes on 14 May 2021.
32. The Uniform and Overseas Citizens Absentee Voting Act, text found on fvap.gov on 14 May 2021.
33. Ura, A.: Here's how Texas elections would change, and become more restrictive, under the bill Texas Republicans are pushing. https://www.texastribune.org/2021/04/21/texas-voting-restrictions-senate-bill-7/ (2021)
34. U.S. Census Burea: QuickFacts Texas; United States. https://www.census.gov/quickfacts/fact/table/TX,US/PST045219, Accessed 13 May 2021

35. Verified Voting Foundation: The verifier. https://verifiedvoting.org/verifier/, accessed on 13 May 2021
36. Wallace, J.: Texas voter turnout was best in almost 30 years. https://www.houstonchronicle.com/news/election2020/article/Texas-voter-turnout-was-best-in-almost-30-years-15705990.php (2020)
37. Wilkie, J.: America's new voting machines bring new fears of election tampering. https://www.theguardian.com/us-news/2019/apr/22/us-voting-machines-paper-ballots-2020-hacking (2019)

A Interview Prompts

- Can you please tell me a little bit about yourself and your responsibilities at Bexar County?
- What are the sources for voting processes and procedures do you have for your region?
- What type of voting system is used in your precinct?
- When does your precinct start preparing the elections? Finding and taking care of vulnerabilities?
- What process does or did your county take to prepare for the 2020 elections? How was your county's process different from the 2016 election for the 2020 election?
- What steps do you follow to test your equipment prior to elections?
- What methods do you use to backup voting counts or results?
- What is your process to deal with equipment security?
- What procedures do you employ to protect voter information?
- In the 2020 elections, did you encounter any specific problems with your voting machines? If yes, what were the problems?
  - What was done to resolve the problems found in the systems? Is there a procedure in place for this?
  - After resolving the problems, what did you learn from this? What should have or needs to be done better?
- Do you have a special organization that deals with election security? Can you tell me about it?
- Overall, would you say that your county is well equipped to secure the voting systems and voter information from cyberattacks?
  - Please explain.
  - If not, what is needed in order to better safeguard voting systems or voter information?