May 10, 2018

The Honorable Rolando Pablos
Secretary of State
1100 Congress
Capitol Bldg., Room 1E.8
Austin, Texas 78701

Keith Ingram, Director of Elections
Secretary of State, Elections Division
James E. Rudder Bldg.
1019 Brazos St.
Austin, Texas 78701

CC: The Honorable Bryan Hughes, Chair, Senate Select Committee on Election Security
The Honorable Jane Nelson, Chair, Senate Select Committee on Cybersecurity
The Honorable Giovanni Capriglione, Chair, House Select Committee on Cybersecurity

Re: Cybersecurity and Election Security Recommendations

Dear Secretary Pablos and Director Ingram,

As computer scientists and cybersecurity experts at some of Texas's most preeminent academic and research institutions, we write to outline reasonable, but critical, measures that Texas must undertake to make its elections more secure and reliable. An accurate, secure election system is -- and absolutely must be -- a nonpartisan goal. Nothing could be more critical to our American democracy, or to Texans' faith in the elections process. Below, we lay out four key priorities: (1) updated election security standards and accountability mechanisms, (2) auditable paper trails, (3) mandatory post-election audits, and (4) secure voter registration systems.

Two impending events make outspoken leadership from your office an urgent matter. First, Texas will very shortly receive approximately $23.3 million dollars in federal funding earmarked specifically for improving election security.[1] The money may be used to replace voting equipment with machines that provide a voter-verified paper record, implement a post-election audit system, upgrade election-related computer systems to address cyber vulnerabilities, facilitate cybersecurity training for election officials, or implement cybersecurity

[1] Financial Services And General Government Appropriations Bill, 2018, Omnibus Agreement Summary, *available at* https://www.appropriations.senate.gov/imo/media/doc/FY18-OMNI-FSGG-SUM.pdf; Brennan Center for Justice & Verified Voting, *Federal Funds for Election Security: Will They Cover the Costs of Voter Marked Paper Ballots?* (Mar. 2018), *available at* https://www.verifiedvoting.org/wp-content/uploads/2018/03/Federal_Funds_for_Election_Security.pdf.

best practices for election systems.[2] It is crucial that this funding be spent effectively and as part of a comprehensive plan for updating and securing Texas's election systems.

Second, under the Texas Cybersecurity Act, the Secretary of State's office must conduct a study of cyber attacks on election infrastructure by December 1, 2018.[3] We understand that Director Ingram is spearheading this process. The study must include an investigation of vulnerabilities and risks for a cyber attack against Texas's voting and voting registration systems, information on any attempted cyber attack on these systems, and "recommendations for protecting a county's voting system machines and list of registered voters from a cyber attack."[4] As cybersecurity experts and Texas voters, we feel a duty to ensure that your recommendations reflect the best research and analysis of existing technology and its vulnerabilities.

Election security represents a profound challenge to both our democracy and our national security -- one we are confident Texas can meet with its typical innovative spirit. Other states are addressing this challenge with creative policy solutions[5]--but Texas still has an opportunity to be a leader. We urge you to use the mandated report as an opportunity to recommend meaningful and technically-sound updates to our state's systems -- and, if necessary, use your statutory authority to issue updated voting systems standards. Below, we offer four specific policy recommendations that will improve the security, reliability, and transparency of Texas voting and voter registration systems. Some of these represent critical improvements that must be implemented with all due haste.

BACKGROUND

Texas's 254 counties employ an array of election systems, with voting methods ranging from hand-marked paper ballots to direct-recording electronic (DRE) voting machines. In the 2016 election, approximately 148 counties used some or all paperless DRE machines, which produce no auditable paper trail.[6] This includes Harris County, which has over 2.2 million registered voters and uses entirely paperless DRE machines for election day voting.

A number of the machines currently employed in Texas have known security vulnerabilities, exacerbated by lack of an auditable paper trail.[7] Our state's voting machine

---

[2] Staff of H. Comm. on Appropriations, 115th Cong., Joint Explanatory Statement on Financial Services and General Government Appropriations Act, 2018 (2018), http://docs.house.gov/billsthisweek/20180319/DIV%20E%20FSGG%20SOM%20FY18%20OMNI.OCR.pdf.

[3] Tex. Elec. Code § 276.011(a)(1).

[4] Tex. Elec. Code § 276.011(b)(1)-(3).

[5] Bennett Leckrone, *Ohio Senate OKs $115 million to help counties replace voting machines*, The Columbus Dispatch (April 12, 2018), *available at* http://www.dispatch.com/news/20180412/ohio-senate-oks-115-million-to-help-counties-replace-voting-machines; Press Release, "Department of State Tells Counties to Have New Voting Systems in Place by End of 2019" (April 12, 2018), Pennsylvania Department of State, *available at* http://www.media.pa.gov/Pages/State-Details.aspx?newsid=276.

[6] Verified Voting, *The Verifier - Polling Place Equipment - November 2016*, *available at* https://www.verifiedvoting.org/api?advanced&state_fips=48&equip_type=&make=&model=&year=2018&download=excel.

[7] *See, e.g.*, Adam Aviv *et al.*, *Security Evaluation of ES&S Voting Machines and Election Management System*, *available at* https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf (ES&S iVotronic interface);

security is further undermined by the age of the equipment in use today. Equipment in many Texas counties is over a decade old. For example, Bexar County's 2,842 DRE machines, which have no verifiable paper trail and serve over 1 million registered voters, were purchased in 2002.[8] We must assume that adversaries have had plenty of time to devise attacks on these machines, many of which are obsolete. In some cases, manufacturers no longer make replacement parts or provide security updates for critical components. Texas voter registration systems -- forty separate databases in total -- are particularly vulnerable as they are networked and largely unregulated at the state level.

It is no longer sufficient to rely on physical protection of our election infrastructure: secure elections require "defense in depth" to ensure that they can be robust in the face of misconfigurations, misunderstandings, and malice. Texans deserve modernized and cyber-secure voting systems. It is time to plan for the necessary expense of retiring Texas's outdated and insecure voting technology, and replacing it with equipment that better satisfies cybersecurity best practice standards. This will take forethought, and it will take legislative and executive action. The security concerns described below are very real, and it is important that Texas proceed to address them.

Although our current voting systems are aging and insecure, Texas must balance the need to act quickly with the need to ensure that new systems meet better standards than are currently in place. Our state leaders, including your office, must prioritize smart and forward-looking expenditures grounded in the best available research. Like any essential state function, there is a cost to securing Texas elections. But the cost is not insurmountable, and it is money very well spent. As an initial matter, the recently-allocated federal funding, if deployed effectively, can help with short-term planning and preparations between now and the November 2018 election.

RECOMMENDATIONS

Below, we lay out four specific policy recommendations that will improve the security, reliability, and transparency of Texas voting and voter registration systems. As a general matter, we see two overarching priorities: improving statewide standards to ensure election security going forward, and replacing Texas's aging, outdated, and vulnerable voting systems in conformance with these standards. ***The order of operations here matters***: there must be improved standards in place before new voting machines are purchased. The reason is simple: if we allocate money before standards are in place, counties and the state will invest significant resources on inadequately secure voting machines that will, for all practical purposes, be

---

Matt Blaze & Jake Braun, *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* (Sept. 2017), *available at* https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf (Premier AccuVote TSx, ES&S iVotronic interface); Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine* (2006), *available at* https://s3.amazonaws.com/citpsite/publications/ts06full.pdf.

[8] Jacquelyn Callanen, *How Bexar County elections officials protect Texans' votes*, Trib Talk, a publication of the Texas Tribune, (Oct. 24, 2016), *available at* https://www.tribtalk.org/2016/10/24/how-bexar-county-elections-officials-protect-texans-votes/.

grandfathered in under the current standards.[9] The problems identified above will be replicated for another decade -- or more. This reality deserves especial emphasis in light of Texas's imminent receipt of federal funding from March's omnibus federal spending bill.

These recommendations are based on our collective expertise, years of research, and best practices articulated by leading independent research organizations. Together, these recommendations describe a system of election administration that provides reasonable cybersecurity. We urge you to include these recommendations in your report to the Legislature on December 1, 2018, and to use your statutory authority to ensure that as many of these changes are in place as early as possible. We stand ready to lend our expertise to the drafting and implementation of updated standards.

1. **Your office, and the Legislature, should design and implement protective and proactive election cybersecurity standards and accountability mechanisms that ensure statewide compliance with best practices.**

Laws and regulations must be in place to ensure consistent cyber-hygiene throughout Texas's election system. This includes not just voting machines, but voter registration systems, electronic poll books, IT infrastructure, and any other system whose disruption could alter the vote, alter who is able to vote (e.g., by changing registration records), sow confusion on election day (e.g., by causing machines to crash), or otherwise undermine Texas's ability to hold fair and reliable elections. You need not start from scratch; independent research organizations have developed comprehensive best practices that need only be translated into regulatory language.[10] Many of these standards can and should be in place before the November 2018 election.

Two narrow but necessary improvements are worth mentioning here. First, the State of Texas does not currently require election officials to undergo cybersecurity training. Last year's Verizon's Data Breach Investigation Report (DBIR), which analyzed 1,935 actual security breaches reported by sixty-five partner organizations, noted that "1 in 14 users were tricked into following a link or opening an attachment—and a quarter of those went on to be duped more than once" and "80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords."[11] Untrained or careless end-users are typically the greatest security vulnerability. Even otherwise tech-savvy users can be manipulated into compromising a network if they lack proper security awareness. Texas should require cybersecurity training for county and local election officials so that they aren't tricked into allowing bad actors into county and state systems.

---

[9] *See* Tex. Elec. Code §§ 122.001(a)(3), 122.031(a), 122.032(a); 1 Tex. Admin. Code §§ 81.60, 81.61.

[10] For example, see Verified Voting Foundation, Principles for New Voting Systems, *available at* https://www.verifiedvoting.org/voting-system-principles/ (listing ten key principles to which every voting system should conform); Center for Internet Security, A Handbook for Elections Infrastructure Security (Feb. 2018) at 36-66, *available at* https://www.cisecurity.org/elections-resources/ (detailing best practices to address risks to elections systems, categorized by priority (high to low), cost, and connectedness class (network connected, indirectly connected, or transmission)).

[11] 2017 Verizon Data Breach Investigations Report (10th Ed. 2017), *available at* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Second, Texan voters stationed or living overseas must not be allowed to return voted ballots electronically, as is currently allowed for overseas military voters in Bexar County. As Professor Dan Wallach testified on February 22, the Internet "makes it much easier for nation-state adversaries to attack our elections . . . . Safe internet voting is simply not feasible today. . . particularly in light of the threats these systems will face."[12] There is presently no way to economically and adequately secure votes submitted online--but there are other ways to ensure Texas military members are able to vote.

In addition to a legislative solution, your office can prescribe additional standards for voting systems beyond the basic requirements laid out in Texas Election Code § 122.001(a). The standards can apply to particular kinds of voting systems, particular elements comprising a voting system, or to voting systems generally.[13] At the earliest practicable time -- but no later than necessary to implement improvements in advance of the 2020 election -- we urge you to use this statutory authority to ensure that Texas voting systems meet the highest possible cybersecurity standards.

Additionally, the legislature should grant the Secretary of State sufficient authority to ensure that *all* Texas voters enjoy access to voting systems equipped with adequate safeguards. As Director Ingram repeatedly testified at the Senate Select Committee on Election Security's February 22, 2018 hearing,[14] the Texas Secretary of State lacks the authority to enforce substantive provisions of the Election Code. Although legislative solutions are necessary, updated election security requirements will be meaningless if there is no way to hold counties -- and vendors -- accountable for compliance. There must be a system in place to ensure that modernized, effective standards are uniformly followed. Therefore, we suggest your recommendations include a provision allowing the Secretary of State's office to enforce the standards issued by that office as well as those provisions of the Election Code governing election equipment, voter registration, and cybersecurity training. To this end, your office should also recommend a provision requiring that voting system manufacturers notify the Secretary of State of known security breaches and malfunctions, and provide a penalty for failing to do so.[15]

2. Texas should immediately adopt voting systems standards that require a paper record of every vote cast in every election in Texas, and replace paperless machines with machines that produce a voter-verified paper record.

---

[12] *Hearing Before the S. Select Comm. on Election Cyber Security*, 85th Interim Sess. (Tex. 2018) (statement of Dr. Dan Wallach, Professor of Computer Science, Rice University), *available at* https://www.cs.rice.edu/~dwallach/pub/texas-senate-feb2018.pdf.

[13] Tex. Elec. Code §§ 122.001(c), 122.032(b).

[14] Video Recording: Hearing Before the S. Select Comm. on Election Cyber Security, 85th Interim Sess., (Tex. 2018), *available at* http://tlcsenate.granicus.com/MediaPlayer.php?view_id=44&clip_id=13172.

[15] In early 2018, Washington State introduced legislation that would require manufacturers of voting system equipment to report certain security breaches on their equipment to the Secretary of State and State Attorney General. 2017 WA H.B. 2388. If a voting system manufacturer fails to meet this notice requirement, the Secretary of State must decertify that manufacturer's voting systems. The proposed law also gives the Secretary of State power to decertify a voting system and withdraw authority for its future use or sale in the state if, at any time after certification, the secretary of state determines that it fails legal requirements. *Id.* Colorado requires similar notice of malfunctions; failure to provide notice is grounds for decertification. 8 Colo. Code Regs. § 1505-1:11.

Every vote cast in Texas should produce a voter-verified paper audit trail ("VVPAT") that becomes the official record of the vote cast in the case of a recount or dispute. Paper records (collected in a secure, private way) are indispensable to a secure elections system. A much-touted defense against cyberattacks is the "air gap" around physical infrastructure that physically separates equipment from the Internet. Indeed, Texas should mandate that all infrastructure is truly air-gapped, and that no remote access software has been installed on machines or pollbooks. However, even those voting machines with a physical "air gap" are not impenetrable against unauthorized or malicious access. To the contrary, nation state adversaries have devised a number of workarounds, which have been used to, for example, damage nuclear centrifuges that use similar air gap defenses.[16] Election management software may be an especially viable attack vector.[17] The best mitigations we have for the systems Texas uses today are only possible where there is a paper voting record.

If voting machines in any of the 148 Texas counties that still either fully or partially rely on paperless DRE machines were attacked, it is very unlikely that they would show any evidence of it. By way of example, in the recent Dallas Democratic primary for District Attorney, if merely a handful of the county's 1,250 iVotronic DRE machines were compromised, the outcome (a 584 vote margin out of 112,701 cast[18]) could have been swung in either direction. While no such attacks in that race are suspected, in the event that allegations were made, the Dallas County Elections Department would have been unable to verify the outcome with meaningful certainty. Similarly, in a special election held recently in Pennsylvania's 18th Congressional District, the Republican candidate lost by 758 votes out of over 227,000 cast.[19] Had either side sought a recount, it would not have been possible to conduct a meaningful one due to the lack of any paper trail. Maintaining paper ballot records as a backup is key to election legitimacy: where machines or systems have been attacked, paper ballots provide a far more secure and easily audited record of the vote.[20]

VVPAT can take many forms: an old-fashioned paper ballot filled out by hand; paper ballot filled out by the voter and tabulated by an optical scanning machine; or a printed receipt of votes cast on a DRE machine that the voter uses to confirm that his or her vote was cast correctly. In whatever form, VVPATs safeguard against cyberattacks by providing a non-digital

---

[16] *See, e.g.*, Ralph Langner, To Kill A Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve (Nov. 2013), *available at* https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.
[17] Eric Chabrow, *Intelligence Panel Learns How to Hack Air-Gapped Voting Systems*, Bank Info Security (June 21, 2017), *available at* http://www.bankinfosecurity.com/intelligence-panel-learns-how-to-hack-air-gapped-voting-systems-a-10030.
[18] Tasha Tsiaperes, *There Will Be No Recournt in the Dallas DA Democratic Primary*, Dallas Morning News (March 20, 2018), *available at* https://www.dallasnews.com/news/2018-elections/2018/03/19/will-no-recount-dallas-da-democratic-primary.
[19] Wes Venteicher, *Conor Lamb's lead grows as special election review continues*, Trib Live (March 20, 2018, 4:15 PM), *available at* http://triblive.com/local/regional/13443796-74/conor-lambs-lead-grows-as-special-election-review-continues
[20] Michael Miller, *How the U.S. can prepare for a major election hack*, The Washington Post (March 15, 2018), *available at* https://www.washingtonpost.com/news/monkey-cage/wp/2018/03/15/how-the-u-s-can-prepare-for-a-major-election-hack/?utm_term=.5e3de8bd1f13&wpisrc=nl_politics&wpmm=1.

artifact reflecting the voter's intent that can be subject to audits and recounts as needed to ensure that election results are accurate. However, importantly, paper ballot and optical scanner-based systems are considerably less expensive than DRE-based systems: last year Cameron County replaced its aging equipment with paper ballots and optical scanners for about $12 per registered voter.[21] Based on our examination of recent purchases in eight Texas counties, the total cost of new DRE voting machines averaged $16.42 per registered voter. Operating costs for optical scan machines are also typically lower.[22]

There are two realistic, more secure voting machine options available today. First, *next-generation optical scan systems*, specifically precinct-based optical scan systems. These systems involve hand-marked ballots that are scanned at the ballot box. Although optical scan systems face cyber threats, paper ballots enable robust paper audit procedures. Some Texas counties, Denton County included,[23] already use this technology.

Second, *next-generation hybrid voting systems*, such as Los Angeles County's Voting Systems Assessment Project and Travis County's STAR-Vote,[24] generate printed paper ballots which can be tallied electronically or by hand. These systems use sophisticated cryptographic security techniques[25] and allow for risk-limiting audits,[26] described in more detail below. A key benefit of bespoke systems like these is that the hardware (the physical machine, including screen and printer) and voting software are unbundled; software can be updated without purchasing new equipment (and vice versa), and off-the-shelf hardware can be repaired with commercially-available products. Texas is a great engine for innovation in many fields, and the field of voting technology need be no different.

---

[21] The total cost of the new machines was $2.5 million in Fall 2017, and Cameron County had 201,020 registered voters as of March 2018. *See* Frank Garza, *New Voting Machines to be More Efficient, Secure*, The Brownsville Herald (Oct. 7, 2017), *available at* http://www.brownsvilleherald.com/premium/article_ebdc8660-abcf-11e7-9900-6f329a8b88e1.html; Texas Secretary of State, *March 2018 Voter Registration Figures*, *available at* https://www.sos.state.tx.us/elections/historical/mar2018.shtml.

[22] Verified Voting, "Are verified paper ballots cost effective?", *available at* https://www.verifiedvoting.org/downloads/Newvvpbcosts.pdf.

[23] Emma Plattoff, *Denton County going to all-paper ballots for November*, Star-Telegram (July 4, 2017, 2:14 PM), *available at* http://www.star-telegram.com/news/politics-government/election/article159587389.html.

[24] *See* Voting Systems Assessment Project: Phase III: System Design and Engineering (2017), *available at* http://vsap.lavote.net/wp-content/uploads/2017/08/VSAP-Phase-III-Report.pdf; Susan Bell *et al.*, STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System (2013), *available at* http://traviscountyclerk.org/eclerk/content/images/presentations_articles/cuc_presentation/pdf_tc_elections_8_dans_star2013_presentation_paper.pdf. For more details on how STAR-Vote works, see a video and technical paper at https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell.

[25] What can sophisticated cryptography do? Cryptography, used properly, provides mathematical transformations of ballots that can protect the privacy of votes while simultaneously allowing any election observer to verify that votes were "counted as cast" (i.e., that the individual votes, posted in public, add up to the correct totals) and that the votes were "cast as intended" (i.e., that potentially malicious voting machines would be caught if they tried to substitute votes for other candidates than the voters intended).

[26] *See, e.g.*, Mark Linderman & Philip B. Stark, *A Gentle Introduction to Risk-limiting Audits*, IEEE Security And Privacy, Special Issue On Electronic Voting (Mar. 2012), *available at* https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

One option your office could consider recommending is centralizing the creation and management of innovative and cost-effective voting systems in the vein of STAR-Vote. While there are some benefits to a decentralized system where each county independently purchases and manages its voting systems, centralization would enable significant cost savings, facilitate maintenance and customization, make replacing failed or obsolete equipment much easier, improve security and reliability, and allow for quick and affordable adoption of technological improvements. Moreover, if the design, data formats, and programming interfaces are sufficiently open, there can be a competitive market for support services, including configuration, maintenance, integration, and customization.

Both optical scan and hybrid systems conform with independently-developed best practices for modern voting systems.[27] ***Most importantly, whatever machines Texas adopts must provide voters with the means and opportunity to verify human-readable marks on paper that correctly represent their intended selections, before casting their ballot, and preserve vote anonymity.*** Ideally, Texas voting systems should be such that county elections officials should be able to configure, operate, and maintain the system, create ballots, tabulate votes, and audit the accuracy of the results without relying on external expertise or labor, even in small counties with limited staff.

3. Texas should require post-election audits for all elections in all jurisdictions and, in particular, implement the best practice of risk-limiting audits.

Texas should require mandatory post-election audits,[28] with clear rules for the methodology and size of the audits, and the point at which audit results trigger a larger audit or full-scale recount. Currently, Texas law only requires post-election audits in jurisdictions using paper ballots.[29] The law also provides the Secretary of State with discretion to audit in jurisdictions using electronic voting systems.[30] This is manifestly insufficient in today's cyberthreat environment. Like VVPATs, clear and rigorous audit procedures safeguard against hacks by creating a statistically-sound method for detecting anomalies and a policy for overriding electronic tabulations if they become unreliable. It bears emphasis that ensuring appropriate audit practices means also ensuring that all jurisdictions use VVPATs. Without a paper record, meaningful audits are impossible.

---

[27] *See, e.g.*, Verified Voting Foundation, Principles for New Voting Systems, *available at* https://www.verifiedvoting.org/voting-system-principles/.

[28] In 2017, Colorado became the first state to implement mandatory risk-limiting audits. *See* C.R.S.A. § 1-7-515 (2)(a). Rhode Island subsequently passed a bill mandating risk-limiting audits beginning in 2020. 17 R.I. Gen. Laws § 17-19-37.4. Other states, including California, Oregon, and Utah, require mandatory post-election audits. *See, e.g.*, Cal. Elec. Code § 15560; O.R.S. § 254.529; Office of the Lieutenant Governor, "Election Policy," § 6.2 (Oct.17, 200), *available at* https://www.verifiedvoting.org/wp-content/uploads/2017/03/ElectionXPolicy.pdf.

[29] Texas law requires that the audit is done by a "manual count." Tex. Elec.Code § 127.201(a). However, many Texas precincts use direct-recording electronic machines (DREs) without a voter-verified paper audit trail (VVPAT), meaning that no hand count of ballots or VVPATs can be conducted in those precincts. And indeed, the audit statute explicitly provides that the hand count requirement does not apply where DREs are used. *See* Tex. Elec. Code §127.201(g).

[30] Tex. Elec. Code § 43.007(c).

In particular, the clear best practice is to require risk-limiting audits of the sort now required in Colorado.[31] This procedure increase voter confidence that election outcomes are correct and can help counties discover and correct procedural mistakes. A risk-limiting audit is an "audit protocol that makes use of statistical methods and is designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome."[32] The number of ballots included in an audit should be a statistically significant number tied to the margin of victory, not a fixed number as currently called for under Texas law. [33] To be at all meaningful, audits should be binding on the outcome of elections, and the discovery of an error should have an impact.

4. Voter registration systems, a weak link in Texas's election security, should be certified as secure, redundant, and accurate.

There are numerous threats to Texas's hybrid voter registration system, which aggregates thirty-nine locally-managed county databases with additional data from the 215 counties that are centrally managed. This hybrid system stores the records of over fifteen million voters. In many ways, this system represents the most critical and scalable target of our election infrastructure, because it includes 100% of the potential votes in any Texas election. As Senator Marco Rubio recently highlighted in a U.S. Senate Select Committee on Intelligence hearing, a foreign power could "penetrate the voter database of local election officials and strategically located counties or states, and . . . go into the database and they change the addresses of individuals, thereby their precincts move around, maybe they even delete some people from the rolls."[34]

Even a redesigned voter registration system would still, by necessity, require Internet connection so voters can verify their correct polling places, see sample ballots, and so forth. Most notably, during Texas's early voting period, we need an online database to track which voters have cast ballots. The mere fact that voter registration databases are network-connected (that is, online) results in a significant increase in vulnerability and risk. There are well known best practices to mitigate these risks, but "the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components."[35] These most vulnerable links in Texas's election security chain must be strengthened as soon as is practicable.

---

[31] Colorado Secretary of State, Understanding Risk Limiting Audits, *available at* https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/UnderstandingRiskLimitingAudits.pdf. *See also* Center for Internet Security, A Handbook for Elections Infrastructure Security (Feb. 2018) at 28-29, *available at* https://www.cisecurity.org/elections-resources/.

[32] Colo. Rev. Stat. § 1-7-515. *See also* 8 Colo. Code Regs. § 1505-1:25 (detailing risk-limiting audit procedures).

[33] *See* Tex. Elec. Code § 127.201(a) ("To ensure the accuracy of the tabulation of electronic voting system results, the general custodian of election records shall conduct a manual count of all the races in at least one percent of the election precincts or in three precincts, whichever is greater, in which the electronic voting system was used").

[34] *Hearing on Election Intelligence Before the S. Select Comm. on Intelligence,* 115 Cong. (2018) (statement of Sen. Marco Rubio), *statements also available at* https://www.rubio.senate.gov/public/index.cfm/press-releases?id=0E99BF69-9CF4-460B-B911-046E7384665F.

[35] Center for Internet Security, A Handbook for Elections Infrastructure Security (Feb. 2018), *available at* https://www.cisecurity.org/elections-resources/.

Certification of Voter Registration and Management Systems

The Legislature must expand the responsibilities of the Texas Secretary of State's role in certifying voting systems to include the certification of voter registration and management systems. Counties that determine that subsequent, necessary security upgrades and practices are too costly could migrate to the statewide system. Specific requirements for such certification might include those listed in the National Research Council's "Improving State Voter Registration Databases,"[36] or the more recent recommendations issued by the U.S. Computer Emergency Readiness Team in their memo "Securing Voter Registration Data" memorandum.[37] The requirements will need to evolve regularly to keep pace with the threat landscape, so a flexible administrative framework that can be regularly updated is preferable to static set of rules/technical specifications.

As initial steps, Texas must establish baseline computer security standards for network firewalls, intrusion detection systems, and other "good hygiene" practices. The state should also consider centralizing the creation and management of voter registration tools, which would allow for more intensive and comprehensive cybersecurity reviews, and might aid in detecting anomalous changes to voter information. And, Texas should consider engaging independent third party vendors to provide ongoing services such as security assessments, vulnerability scanning and patching, penetration testing, and infrastructure monitoring and management.

Disaster Recovery/Continuity Planning

Something as massive as a hurricane or minor as a burst pipe above a server room could derail the administration of an election. Cyber attacks are also a form of disaster, and can have equally catastrophic effects. For example, Atlanta's city services were recently hobbled for a week over a ransomware attack aimed at simply extorting $51,000 in Bitcoins.[38] In the same week, Baltimore's 911 and 311 services were partially disabled by a separate attack.[39]

To mitigate risk from any of these potential events, the state should mandate that all critical server infrastructure related to voter databases (and, indeed, all election-related servers) should be capable of both local and offsite failover (the ability to switch to a redundant system during a failure) and snapshotting (the ability to revert to a previous instance of a system), which should be tested on a regular schedule through mandated drills to ensure counties can rapidly recover from corrupted or offline systems. Offsite encrypted backups of voter registration data should be required weekly. In the case of a ransomware attack, these measures would allow a jurisdiction to restore their affected systems with minimal data loss or services impact. To a

---

[36]National Research Council: Improving State Voter Registration Databases: Final Report (2010), *available at* https://doi.org/10.17226/12788.

[37] United States Computer Emergency Readiness Team, *Security Tip (ST16-001): Securing Voter Registration Data* (Sept. 30, 2016), *available at* https://www.us-cert.gov/ncas/tips/ST16-001.

[38] Leada Gore, *Atlanta Computers Still Down 6 Days After Cyber Attack; Will City Pay Ransom?*, AL.com (Mar. 28, 2018), *available at* http://www.al.com/news/index.ssf/2018/03/atlanta_computers_still_down_6.html.

[39] Kevin Rector, *Baltimore 911 Dispatch System Hacked, Investigation Underway, Officials Confirm*, Baltimore Sun (Mar. 27, 2018), *available at* http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-911-hacked-20180327-story.html.

similar end, jurisdictions that use electronic poll books should also be required to have paper backups at each poll site on election day; this practice is currently voluntary.

CONCLUSION

Our voter registration, vote casting, and vote tabulation systems are not ready to rebuff attacks from nation-state adversaries or others determined to attack the accuracy of Texas elections. Concrete steps must be taken to shore up Texas's elections systems as soon as possible, and certainly before the 2020 election. Under the Texas Cybersecurity Act, your office has a key role to play: your recommendations, due on December 1, and your advocacy in support of meaningful action in the 2019 legislative session, can be instrumental in turning Texas into a model for secure, accurate, and fair elections.

We urge to ensure that any federal funding Texas receives is spent wisely and in accordance with the principles outlined above. We also urge you to include the above recommendations in your December report. Of course, each one of these recommendations could be the subject of a lengthy and technical memorandum explaining best available practices. Texas has a wealth of expert resources, including the undersigned, and we urge you take advantage of this fact by engaging with computer security, cybersecurity, and election infrastructure experts to hone the specific language of your recommendations over the course of the next seven months.

Texans deserve an election system they can trust. The federal Constitution gives states authority over the conduct of elections, and few of our state's responsibilities go more directly to the heart of our democracy. As Texans and computer scientists, we stand ready to assist in designing and implementing reasonable changes that will make a significant and lasting difference -- and make Texas a leading example of reliable, accurate, and secure elections practices.

For inquiries regarding this letter, please contact Dan Wallach <dwallach@rice.edu>, 713-348-6155.

Sincerely,

Scott Aaronson, Professor, University of Texas at Austin

Chris Bronk, Assistant Professor, University of Houston

Alvaro Cardenas, Assistant Professor, University of Texas at Dallas

Guofei Gu, Associate Professor, Texas A&M

Murat Kantarcioglu, Professor, University of Texas at Dallas

Jiang Ming, Assistant Professor, University of Texas at Arlington

Dan S. Wallach, Professor, Rice University

Brent Waters, Associate Professor, University of Texas at Austin

Greg White, Professor, University of Texas at San Antonio

*****_In alphabetical order; affiliation given for identification purposes only._