



THE EAC'S BEHAVIORS, LAX STANDARDS AND APPARENT ALLEGIANCES TO VOTING MACHINE VENDORS PROVE THEIR MACHINE CERTIFICATION PROCESS IS UNTRUSTWORTHY

Executive Summary

The apparent close relationship between the Election Assistance Commission (EAC) and the voting machine vendors they are supposed to hold in check makes their performance ensuring those machines are free of potentially nefarious software/hardware and trustworthy, questionable at best. The EAC's membership, leadership and recent out-of-the-spotlight moves to allow machines to now have internet access flies completely in the face of their stated purpose and makes them dubious in how they are protecting citizens. Their moves also show that recent election officials' adamant statements that voting machines "aren't connected to the internet" is now bogus. Additionally, their limited number of approved firms to conduct certification/decertification audits is problematic and the fact that Tennessee's Secretary of State requires all voting machines used in Tennessee be first certified by the EAC demands the recommendation for Tennessee to find another outlet for both certification of machines and identification of standards by which voting machines manufacturers should abide. One that consumers can trust.

Issues

A government entity created by the [2002 Help America Vote Act, the Election Assistance Commission's](#)¹ (EAC) main purpose is, primarily, to oversee and guide voting equipment manufacturers in the development of machines that are safe, secure and trustworthy by the public and test the machines to be sure they meet certain standards – the [Voluntary Voting System Guidelines](#).² However, it is now apparent that the EAC has not made good on that pledge to ensure machines are secure as subsequent election experts, studies, documentaries, affidavits and data studies both before and following the 2020 election have proven. Congressional testimony and the statements of Congressmen and women long before the 2020 election additionally attest to this.

Current machine providers will not be openly transparent and attest to the safety and security of their machines despite the calls from the public and government officials to do so. Where is the EAC seeking to be transparent? Vendors have refused to answer our questions about their machinery. In fact, some vendors have openly attacked officials and citizens who have raised questions seeking nothing more than to ensure machines are incapable of being hacked or votes counted by them incapable of being changed by nefarious bad actors.

- The EAC recently voted against its own security recommendations and the recommendations of its Board, the Standards Board and public comment and has now approved vendors to allow internet connectivity on voting machines. One of its Board members has resigned because of this and is suing the ERC for this action. Why is the EAC now refusing to provide greater security for voters?

¹ <https://www.eac.gov/about-the-useac>

² <https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines>

- The EAC has done little to dispel the notion that their certification process is being deceptively used by vendors as a seal of approval and attainment of the latest in security standards when no vendor today is certified to criteria past 2005 EAC standards.
- A closer look at the EAC's leadership and membership show a cozy relationship with machine vendors and entities that refused to sincerely look at the empirical evidence of 2020 voting issues with machines... instead, proclaiming the election "the most secure in American history" despite evidence to the contrary. The EAC continues today bending toward machine vendors instead of toward consumers/citizens.
- Concerning the EAC's process for certifying vendor machinery there are only two firms in the nation that have been approved by the EAC to test voting systems. And one of these firms dedicated to such security sports a completely unsecure website touting its services.

One doesn't have to be an expert in election machinery to know these are significant issues that raise concerns. And the fact that the EAC does not appear to be doing anything in the way of taking a stand that ensures the purity and trustworthiness of American elections tells us that the EAC is nothing more than a paper tiger and other resources in this arena must be found.

Discussion

Formed in 2002 as a part of the nation's Help America Vote Act, the Election Assistance Commission (EAC) was established to develop guidance to meet the requirements of the Help America Vote Act, adopting voluntary voting system guidelines, as well as accrediting testing laboratories and certifying voting systems. The EAC is advised by a [Standards Board](#)³ and a [Board of Advisors](#).⁴ The [Technical Guidelines Development Committee](#)⁵ was also established to assist the EAC in the development of [voluntary voting system guidelines](#),⁶ a set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards of VVSG 1.0, which was unanimously adopted on December 13, 2005.

The EAC is also to produce an annual report to Congress and hold public meetings and hearings to inform the public about its activities.

According to the [National Conference of State Legislatures \(NCSL\) August 6, 2018 publication "Voting System Standards, Testing and Certification,"](#)⁷ each state sets its specific standards for voting systems in statute and/or administrative rule. These can be based on the voluntary standards set by the EAC, or not. [At this point, Tennessee requires all vendors first be certified by the EAC](#)⁸ before they can be certified by the State Election Commission for use in Tennessee.

³ https://www.eac.gov/about_the_eac/standards_board

⁴ https://www.eac.gov/about_the_eac/board_of_advisors

⁵ https://www.eac.gov/about_the_eac/technical_guidelines_development_committee

⁶ <https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines>

⁷ <https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx>

⁸ https://sharetn.gov.tnsosfiles.com/sos/election/minutes/20151201_SECMInutes_VotingMachine.pdf

The most common issues that voting system standards address are: security, functionality, privacy, usability, and accessibility. Currently, though, citizens are most concerned with the issue of security. And, unfortunately, all vendors – as well as the EAC -- appear to be failing the security standard and afraid to address the primary concern of consumers/citizens.

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

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

But from our research, we’ve found:

- Physical security of the equipment and ballots: [Both the machinery and ballot processes in Tennessee are weak.](#)⁹ And [cybersecurity experts agree with this completely.](#)¹⁰
- Auditability: [DREs and ballot marking devices – all technology/machines for that matter -- we know are especially susceptible to hacks.](#)¹¹ And in Tennessee, that affects at least 70 percent of Tennessee counties – approximately 2.6 million Tennesseans (or 59%) – whose votes can’t be audited because there are no paper ballots produced by DREs and separate from the machines. Votes on these machines are locked inside under the direction of the software.... software that we know can be hacked. This is a huge risk to election integrity.
- Internet connection: It has been proven via studies, presentations and various information sources across the nation [that voting machines – even those approved by the EAC -- can be hacked](#)¹² and in 2020 were, in many cases, connected to the internet. In fact, [Dominion’s own president has admitted as such for his machines.](#)¹³ So, since forensic audits aren’t allowed at this point to prove consumers wrong and vendors right, how can we be sure that machines weren’t connected to the internet? We can’t. We have to look at what we know in the fuller context.

Several of our team attended the July 12, 2021 meeting of the Tennessee State Election Commission (SEC) where two voting machine vendors (Hart and ES&S) demonstrated their upgraded machines for SEC approval. We asked several questions of the vendors, some of which they couldn’t answer. So, we wrote our questions – many of which concerned security issues about the machines – and sent them to the vendors. One response came back refusing to answer our questions because we weren’t election officials. Believing that all vendors would do the same, we compiled our questions for all five vendors

⁹ <https://www.npr.org/2019/09/04/755066523/cyber-experts-warn-of-vulnerabilities-facing-2020-election-machines>

¹⁰ <https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/>

¹¹ <https://www.youtube.com/watch?v=3qr67h54V00>

¹² <https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russians.html>

¹³ https://www.theepochtimes.com/some-dominion-machines-can-connect-to-the-internet-ceo-acknowledges_3620741.html

used in Tennessee and placed them in the hands of Mark Goins, Director of Elections in Tennessee, requesting that he obtain answers for us.

That was August 11th. We're still waiting for answers from Mr. Goins.

Here's one of the questions we've asked after studying the Dominion manual and using logic to figure out what could conceivably happen with such a software/hardware arrangement... on Dominion equipment that has been approved as acceptable by the EAC, and, thus, by the Tennessee State Election Commission:

Through a deeper study of the Dominion Result Tally and Reporting (RTR) system found in the latest manual, we have deduced that the system allows for mass vote changing by deleting results previously entered from secure removable media and replacing them with data from a local file... with no dual-party authentication required. We've also seen that reports can be published to "Public" transfer points inferring that there is at least an indirect connection to the internet. Additionally, it seems that remote clients can communicate with the server through Dominion... again inferring a network connection.

We have heard nothing back either from Goins, the Secretary of State's office or Dominion. However, we have heard a frightening answer from the Williamson County Election Commission employees.

In studying the RTR manual, it was plain that the system could allow mass vote changing by voiding results previously entered from secure removable media from the vote tally and replacing them with data from another file or by manual entry. This can be done by a single individual with access to the system and with no dual-party authentication or other oversight required.

Additionally, it appears that the RTR system can be publish results to "Public" transfer points inferring that the RTR system supports at least an indirect connection to the internet and therefore is exposed to hacking. Finally, the manuals state that remote clients can communicate with the server ... again inferring a network connection. Williamson County has assured us that our RTR system is not used for either of these purposes and is in no way connected to the internet.

But in a meeting to inspect the voting machines for several Alderman candidates on September 28, 2021, the individual in the Williamson County Elections office who manages the RTR was interviewed. They indicated that they were, in fact, able to make such a change, but that they would never do so. While we trust that this is true, we feel that the controls protecting against such an action are dangerously inadequate.

Again, keep in mind this machine has been approved by the EAC and the State Election Commission as safe and secure!

We have identified two controls that may prevent such a manipulation from occurring undetected which we understand are currently not in place. They are included in the recommendations our team is making for a best practices pilot in Williamson County:

- A parallel hand tally of voting center, precinct early voting and absentee voting totals confirmed to match the numbers published by the state for our county; and
- A mandatory audit of the RTR/RTM log files, prior to certifying election results. (As an aside, Dominion performed a software update on our system in January '21, it has been reported from other locations that this upgrade writes over the digital log files that would have been written for the 2020 general election. Williamson county currently considers only paper records as election artifacts that must be retained for 22 months after an election. As a result of our queries, they are now asking for clarification as to whether digital records must also be retained.)

So, it appears that thousands of votes could be switched, and the vote totals changed by nefarious actors hacking into the RTR system which is designed to allow connection to the internet. Fortunately, there is currently a trustworthy person at the helm of the RTR in Williamson County.

We don't think performance like this is allowed in equipment that supposedly reflects high election integrity.

Here's another example of poor performance by the EAC and Tennessee State Election Commission involving equipment both have approved as safe and secure.

In a relatively small Alderman election here in Franklin on October 26, 2021, six Dominion scanners in three distinct voting centers (a large voting location that encompasses all county precinct elections so citizens could vote at any of 8 or more voting centers instead of their assigned precinct) [all ceased counting votes sometime during the day](#).¹⁴ The situation caused the Secretary of State to call the election an incomplete election that would have to be resolved the following day by a full recount of all election-day, early and absentee ballots.

The election was later pulled into the state's Elections Office by Tennessee Coordinator of Elections Mark Goins for study by a task force as to what happened. As of early December, there had been no announcement of the task force or any reference to a report that was to be issued about the incident.

[So, if EAC- and SEC-approved Dominion machines can't handle a simple election of 7,300 voters without "glitching," imagine what might happen if this were a state-wide or national election.](#)¹⁵

At this point, with no answers in hand as to why the EAC doesn't force vendors to increase the security standards of their machinery, we have to conclude that **vendors have something to hide since there has been NO move to answer questions about the safety and security of their machines and NO move towards transparency. And since we've been unable to get an answer from Tennessee Coordinator of Elections Mark Goins at this point about the status of those machine questions, we must hold the SEC equally responsible. Since vendors won't address concerns of citizens directly and the SEC and EAC don't appear to be forcing the issue on behalf of citizens, let's look at what can be observed.**

¹⁴ https://www.williamsonhomepage.com/franklin/election-officials-call-for-a-hand-count-of-votes-from-tuesday-s-city-of-franklin/article_29c49a8e-3719-11ec-b3f3-370527d0638a.html

¹⁵ <https://amp.tennessean.com/amp/8564889002>

Recently, the [EAC quietly and without public input, approved changes in voting machinery at the request of vendors that reduces the manufacturers' cost while substantially weakens the security of voting systems](#).¹⁶ Among other changes, the revised VVSG 2.0 standards now permit inclusion of wireless networking devices in voting machines, removes the requirement for voting systems to record external connections and disconnections during voting and removes the requirement for physical locks installed in voting machines. Cost BENEFITS for vendors. Greater SECURITY risks for citizens.

This questionable move cost the EAC one of their most prominent Board Members, Dr. Philip Stark, who has resigned from the EAC's Advisory Board in protest of this secretive move that is contrary to the organization's mission. [He is now suing the EAC and some of the disturbing claims in his lawsuit include](#):¹⁷

- “The EAC incorporated the changes requested by voting machine manufacturers into the final version of the voting system guidelines. The VVSG 2.0, as adopted by the Commission, incorporates several new provisions that reduce the cost to manufacturers while substantially weakening the security of voting systems as compared to the version of the guidelines that was submitted to the Board of Advisors, the Standards Board, and the public.”
- Help America Vote Act (HAVA) prohibits the EAC from voting to adopt final guidelines until it has given both the Board of Advisors and the Standards Board 90 days to review and comment on the proposed guidelines and has “taken into consideration” their comments and recommendations. By letter dated October 2, 2018, a coalition of election security experts submitted comments to the EAC advocating for a complete ban on wireless modems in voting systems.
- Tens of thousands of public comments were submitted during a public notice and comment period advocating to “ban wireless; require hand-marked paper ballots.” The EAC refused to provide these public comments submitted between February 28, 2019 and June 7, 2019 to the Technical Guidelines Development Committee (TGDC) when requested by the committee.
- On October 15, 2019, a coalition of election security non-profit organizations submitted a letter to the TGDC advocating for a ban on wireless modems and internet connectivity in the VVSG and for the first time made the TGDC aware of the volume of comments advocating for a wireless ban that the EAC had withheld.
- In fact, the EAC held private, closed-door meetings with voting machine manufacturers on a weekly basis from July through August of 2020, as evidenced by records disclosed in response to Free Speech For People (FSFP's) Freedom of Information Act (FOIA) request. The lawsuit establishes that the EAC has negotiated the language and terms of regulations directly with

¹⁶ <https://apnews.com/article/business-technology-government-and-politics-voting-cb9169604edba166db394328144c403>

¹⁷ <https://www.wtrf.com/top-stories/activists-sue-federal-agency-over-voting-system-guidelines/>

[voting machine manufacturers in a nonpublic, parallel proceeding violating the principles of transparency and open government.](#)¹⁸

- Despite two separate email requests “addressed to Jerome Lovato, Mona Harrington, and Jessica Bowers of the EAC, Susan Greenhalgh of FSFP requested to join the weekly meetings between the EAC and vendors. The EAC did not respond.”

That says a lot about who the EAC is looking out for.

Security standards are completely ignored by vendors and the EAC seems oblivious to holding them to this new and ever more robust criteria that would ensure greater security for the voting process. So, again, who does the EAC appear to be supporting? Not consumers/citizens. The EAC’s base certification, first formed in 2005, is the highest level of certification they require of vendors. [Even though the EAC developed newer standards in 2015 and again in 2021, the 2005 standards are the ones they certify.](#)¹⁹ They do not demand vendors step up and apply the improved security standards. Why?

Now think about this. The first smartphone – the iPhone – launched in 2007. Those phones, which are no longer supported or certified because they’re out-of-date, meet more current security standards than any voting equipment in the state of Tennessee. Phones in use since that date have received more upgrades, security patches and updates that make them certified to higher standards than our voting equipment. So, where is the EAC advocating, cajoling, pushing, demanding for adoption of higher standards by vendors as per their mission and moving the vendors toward that goal?

And this too. **By allowing vendors to claim certification from the EAC, without mentioning the inadequate 2005 certification standards level, the EAC is allowing the EAC certification claim to be used by vendors as a seal of approval and attainment of the latest in security standards when no vendor today is certified to criteria past 2005 EAC standards.** Who does this help, the citizens or the vendors?

Perhaps one of the loudest pieces of evidence about the EAC is their people. Admittedly, they are small staffed. **But they’re staffed and have Board representation with people who have past allegiances that should concern everyone seeking unbiased checks on voting equipment manufacturers.**

Take [Jessica Bowers](#), for instance, who, according to the EAC website ([which now appears blocked beyond cursory information, yet the information is verified in a November 20, 2020 news article](#)),²⁰ is listed as Acting CIO/CISO and says she manages “voting system testing and certification projects as well as assisting the development of new Voluntary Voting System Guidelines.”

[Bowers was a ten-year Dominion employee who jumped to the Election Assistance Commission in 2019 and oversees the certification process.](#)²¹ She is also the Dominion employee who on October 8, 2018

¹⁸ <https://freespeechforpeople.org/free-speech-for-people-v-united-states-election-assistance-commission/>

¹⁹ <https://www.eac.gov/voting-equipment/certified-voting-systems>

²⁰ <https://themarketswork.com/2020/11/20/the-small-world-of-voting-machine-certification/>

²¹ <https://themarketswork.com/2020/11/20/the-small-world-of-voting-machine-certification/>

appeared before the Tennessee State Election Commission to ask that the state certify Dominion entering Tennessee with their equipment. The SEC did just that, certifying the equipment for use in Tennessee and approving it unanimously, according to SEC minutes. The contract for the equipment to be used in Williamson County was signed September 4, 2019. Bowers possibly shepherded the process for Dominion's entry into Williamson County for a while but left Dominion on May 9, 2019 to join the EAC's voting certification program.

Interesting that the EAC website fails to mention her Dominion ties.

So, the EAC expects us to believe that if there is a problem with the Dominion equipment in Tennessee and the state forces the equipment back through recertification which could involve the EAC, that Bowers or a colleague of hers is not going to certify it... after selling the equipment to the state and then to Williamson and Hamilton counties? The answer to that is probably why the EAC fails to mention her Dominion roles. Common sense says she will not let Dominion be decertified.

Here are others in leadership/[Board of Advisors](#)²² and [Standards Board](#)²³ of the EAC that because of their biased behavior makes them questionable members of the EAC, even though they are supposed to be unbiased and impartial members of an unbiased and impartial organization. In our judgment, this significantly taints the EAC.

- [Brad Raffensperger](#), Secretary of State, Georgia, who has been questioned significantly for his handling of the 2020 election in Georgia that included pre-election changing of voting laws without legislature approval; significant chain of custody violations that almost a year later are still unresolved; continual problems with Dominion machines per Hari Hursti affidavit; videos showing Fulton County poll workers counting votes from trunks pulled from under tables after all other counting was stopped which has yet to be addressed, etc.
- [Reynaldo Valenzuela Jr.](#), Director of Elections, Maricopa County, AZ, who claimed the county's election was secure, despite the results from a forced audit that the county has fought every step of the way.
- [Veronica Degraffenreid](#), Acting Secretary of State and head of Elections in Pennsylvania, who fought State Senator Doug Mastriano, chair of the Intergovernmental Operations Committee who has pushed for a forensic audit in the state.
- [Jim Condos](#), VT Secretary of State, [who called steps by other states to clean up voting standards such as demanding the requirement of Voter IDs \(which are desired by almost three-fourths of the American voting public\)](#)²⁴ and further restricting voting drop boxes which have proven to be problematic with security and chain of custody and condemned those wanting to look into voting concerns as supporting "The Big Lie."
- [Michael Yaki](#), US Commission on Civil Rights, who was sued by the city of San Francisco for illegally lobbying while he was a city Supervisor before he joined the Commission. (To us, this is an issue with his judgment...)

²² https://www.eac.gov/about_the_eac/board_of_advisors

²³ https://www.eac.gov/about_the_eac/standards_board

²⁴ <http://www.jimcondos.com/huffington-post-runs-condos-op-ed/>

- Dean Logan, County Clerk, Los Angeles County, CA, who faced [scorching criticism over problems voters encountered during an election in 2020](#). Supervisor Janice Hahn commented that she, as well as the public, had “lost confidence” in Logan and the system.²⁵
- Gregory Moore, who was the Deputy Political Director for the Democratic National Committee in the late 90s and oversaw the DNC training division and early White House strategic implementation of the 1996 Clinton-Gore re-election campaign.
- Elizabeth Howard, Brennan Center for Justice, one of three lawyers the Soros-backed Arizona Secretary of State Katie Hobbs deployed to the Veterans Memorial Coliseum to observe the Arizona audit. She also signed the [unfounded complaint letter from Democrat-allied nonprofits](#)²⁶ to harass Arizona Senate President Karen Fann.
- Neal Kelley, Orange County CA Registrar, who [disallowed Republicans from establishing ballot drop boxes in last year’s 2020 election in California](#).²⁷ Republicans refused to remove them, saying they were taking advantage of California’s liberal ballot collection law that allows anyone to collect ballots from voters and deliver them to county election offices.
- David Kladney, US Commission on Civil Rights, who has publicly admonished election officials’ efforts to ensure all voters in U.S. elections are rightful voters for supposedly refusing to register voters who may, in fact, be illegal voters.
- Richard Pilger, Election Crimes Branch, US Department of Justice, [who played a role in the Internal Revenue Service \(IRS\) targeting of conservative groups](#),²⁸ resigned his post last November rather than to do his job and investigate potential voter fraud in the 2020 presidential election as requested by US Attorney General William Barr.
- Lawrence Norden, New York State citizen and Brennan Center for Justice member, who has [written extensively](#)²⁹ about forgoing the requirement of voter IDs as a requirement for someone to vote... which, of course, would mean that anyone could vote regardless if they were a U.S. citizen or not.
- Jocelyn Benson, Secretary of State, Michigan, who dramatically changed her pre-election position regarding the importance of signatures as the most secure way to ensure fair and secure elections, unilaterally watering down the signature requirements for the 2020 election and instructing clerks to presume all signatures were valid. The decision was later [ruled invalid](#)³⁰ this year, but it was too late for Michigan to correct her election mistake.

Finally, **the Voting System Test Laboratories (VSTL) program appears to be highly questionable.** These laboratories are the entities that are approved by the EAC to certify, recertify or decertify voting machine vendors and their machines for use or exemption in states. Again, Tennessee requires any machine used in Tennessee to carry the EAC certification... the certification process of which is performed by a VSTL.

²⁵ <https://laist.com/news/voting-problems-march-3-primary-los-angeles-county-registrar-dean-logan>

²⁶ <https://bloximages.newyork1.vip.townnews.com/azfamily.com/content/tncms/assets/v3/editorial/e/90/e9043f2a-a912-11eb-8828-eb4a33f9446b/608af12c47ea6.pdf.pdf>

²⁷ <https://apnews.com/article/los-angeles-fresno-elections-california-santa-ana-be803bfe99f5eb35e17a6ee56315deb0>

²⁸ <https://www.breitbart.com/2020-election/2020/11/09/richard-pilger-linked-to-irs-scandal-resigns-post-at-doj-over-voter-fraud-memo/>

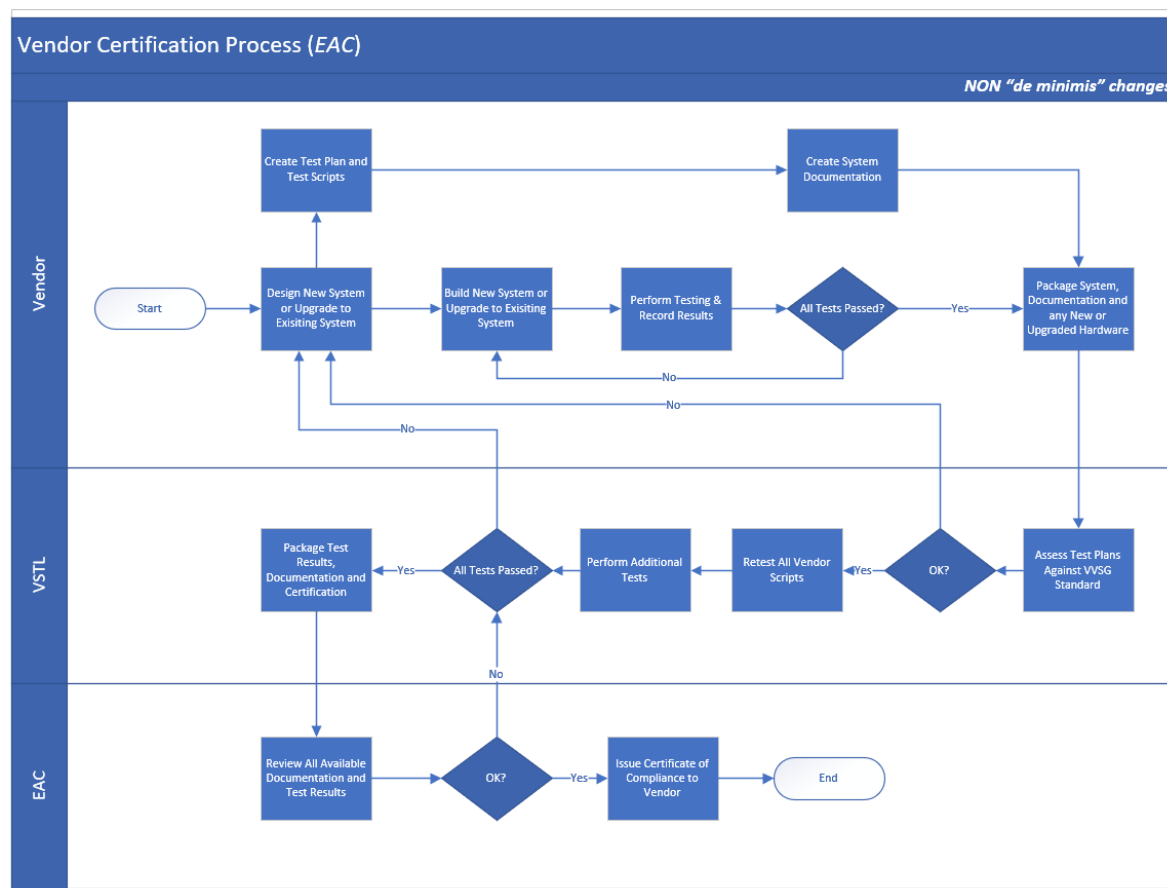
²⁹ <https://www.brennancenter.org/sites/default/files/publications/BCAnnual2012.pdf>

³⁰ <https://www.detroitnews.com/story/news/politics/2021/03/15/judge-rules-secretary-state-bensons-ballot-signature-verification-guidance-invalid/4699927001/>

So, who are these entities? There are only two firms in the nation that have been approved (evaluated and recommended by the National Institute of Standards and Technology) by the EAC to test voting systems to Federal standards.³¹ And one of these firms dedicated to such security – ProV&V³² -- sports a completely unsecure website touting its services.

How does their certification process work? In short, the vendor submits a plan for testing their machinery against 2005 VVSG standards and one of these two firms checks the testing the vendor does to ensure it meets EAC standards. All testing, including functionality testing, is done by the vendors and verified by the VSTL labs. Doesn't sound very aggressive at protecting the public, does it? Neither the EAC or VSTL or vendors publish how – or how rigorously – the machines are tested, or what their process is, and whether there are issues found in the testing. Just whether vendors passed and received EAC certification. We've yet to be able to find a report that is produced to substantiate – or refute -- this process.

We've attempted to diagram the process as we understand it:



³¹ <https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl>

³² <http://www.provandv.com/>

In 2020, [ProV&V tested a software change that Dominion made to machines in Georgia right before the November election](#)³³ and “found no evidence of the machines being tampered” with despite sworn affidavits from poll observers detailing allegations of potential election fraud. But a close examination of Georgia Secretary of State Brad Raffensperger’s October 2, 2020 statements announcing completion of the state’s voting machine audit, indicates the only thing ProV&V did was extract “the software or firmware from the components to check that the only software or firmware on the component was certified for use by the Secretary of State’s office.”

On October 3, 2020, a [counter declaration from Dr. J. Alex Halderman refuted the procedures of ProV&V’s testing](#)³⁴, noting that the “report makes clear that ProV&V performed only cursory testing of this new software. The company did not attempt to independently verify the cause of the ballot display problem, nor did it adequately verify that the changes are an effective solution. ProV&V also appears to have made no effort to test whether the changes create new problems that impact the reliability, accuracy or security of the BMD system.”

So, it appears that the EAC’s vaunted testing firms do not do a thorough, trustworthy job. Where is the EAC dismissing ProV&V or approving other firms to do this work... since they’ve outsourced the job of certification to these entities? Where is the dedication to excellence?

As an aside, the Tennessee State Election Commission says it takes security as seriously as does the EAC – requiring EAC certification to Tennessee machines -- and has an IT expert on staff. But we’ve been unable to learn his/her name, his/her credentials and what he/she does regarding the security standards, the vendors and the machines.

During the July 12, 2021 meeting of the Tennessee State Election Commission where new machine upgrades for Hart and ES&S were approved, [there was no report from an IT specialist that was submitted in person, on paper, or even mentioned to the Commission affirming the machines had been checked for the presence of nefarious equipment changes.](#)³⁵ Yes, the changes were supposedly “De Minimis” changes, but still, in an atmosphere electric with concern from consumers about electronic voting machine vulnerabilities, why was a check of the machines not ordered for any level of change and a report delivered as a part of the SEC’s process? Just to be sure and to let the citizens of Tennessee know the SEC is protecting Tennesseans as the EAC is supposedly protecting Americans?

This is an example of public entities intended to protect the voting security of its citizens not taking the concern of citizens seriously. Of not going the extra mile to be sure citizens are safeguarded from potential fraud. Of not being willing to prove the safety, security and trustworthiness of the product they have been charged to oversee.

³³ <https://themarketwork.com/2020/11/20/the-small-world-of-voting-machine-certification/>

³⁴ <https://apnews.com/article/technology-business-science-voting-election-2020-6755cf1c409f4aab613df8891b84272d>

³⁵ <https://sos-tn-gov-files.tnsosfiles.com/SECAGEND%20-%20July%202012,%202021.pdf?3jGvBK5zy5mgcPY0KRaPdkVy.kZzrHfh>

According to the [Congressional Research Service’s “Insight” publication of February 11, 2021](#),³⁶ as with the Federal Election Commission (FEC) guidance —and in contrast to the mandatory standards in Title III—states are not required to use voting systems that meet the VVSG. Voting systems must comply with the guidelines to receive federal certification, however, and states may choose to make some or all of the federal guidelines, testing, or certification mandatory under their own state laws.

Tennessee needs to do that. The EAC is a paper tiger. Numerous videos and reports that have been submitted from experts (including one notorious 2018 Fundtheaudit.com video that we haven’t submitted, which has probably been seen by millions featuring ten different Democratic representatives, senators and Vice President Kamala Harris) voicing concern about the vulnerability of these machines **should have moved the EAC into fast action to address this serious and seemingly non-partisan issue. But it hasn’t.** Proof that the organization doesn’t care about the public as much as it cares about the vendors.

Our state must change its requirement for EAC certification. After fifteen years, with the industry facing security issues yet the EAC making no more advancements than it has, especially in answer to consumer calls for greater security, the EAC has had plenty of time to prove its value. **Tennessee needs to take the reins of certification to give its citizens greater comfort that election integrity is highly important to the state.**

As we recommended to the Tennessee State Election Commission on October 11, 2021, start right now by establishing a citizen committee composed of cybersecurity and other technology experts much like those we have on our team and establish a Minimum Voting Security Guidelines (MVSG) mapped to the VVSG 2.0 and demand adherence.³⁷ Search the market for a voting equipment firm that shows greater dedication, greater urgency to achieving higher security standards and commit to adhere to those standards and allow them the honor of helping Tennesseans vote. Securely. Is American ingenuity so damaged that there’s not one firm in the marketplace that states can trust and citizens can appreciate for its efforts toward election integrity? We bet a firm is out there that can – and will -- meet our demands.

All voters want is to know their vote counted... that the election was fair and honest... and that the results truly represent the will of the people, whatever that might be. But citizens don’t trust today’s election machinery. And the EAC – and even the Tennessee State Election Commission – are not helping. Changes need to be made to ensure greater election integrity.

Recommendation

We strongly recommend that Tennessee move away from the EAC as a certification entity and find a more trustworthy source to establish standards and conduct certification audits that are consistent with the public’s heightened concerns about the security standards of the equipment used in the state’s elections. Additionally, given the ability today for almost any machinery to be hacked by nefarious characters, we recommend the review and certification processes be stacked with a committee of an

³⁶ <https://crsreports.congress.gov/product/pdf/IN/IN11592>

³⁷ https://www.theepochtimes.com/even-in-red-tennessee-election-integrity-an-uphill-battle_4047323.html

equal number of non-partisan experts in cybersecurity/information technology/process engineering to ensure procedures and equipment are in place to prevent intrusion by nefarious external actors.

Conclusion

Searching the marketplace for alternatives to the EAC and VSTLs is a no brainer. We should start the process immediately.

###