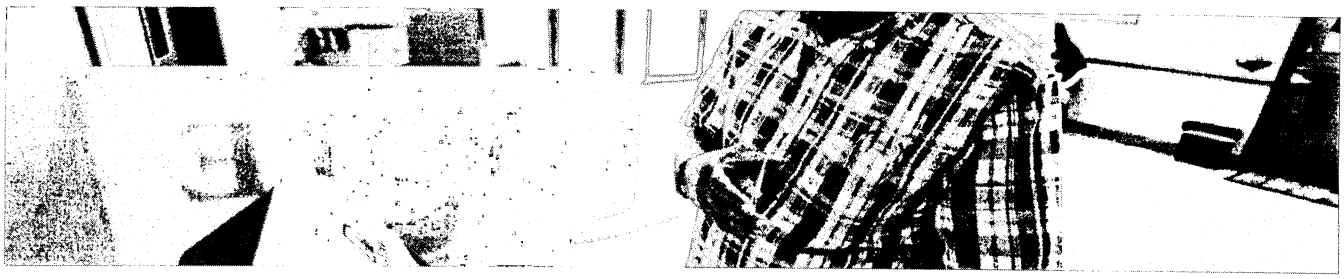


Walter Greene Jr. ponders his vote as Bastrop County election officials host an open house in Cedar Creek, TX, on September 1, 2020, giving a preview of new ExpressVote electronic voting machines slated for the crucial November elections. Photo credit: © Bob Daemmrich/ZUMA Wire

ELECTIONS

Election Assistance Commission Investigated ES&S Voting Systems

JENNIFER COHN 03/08/21

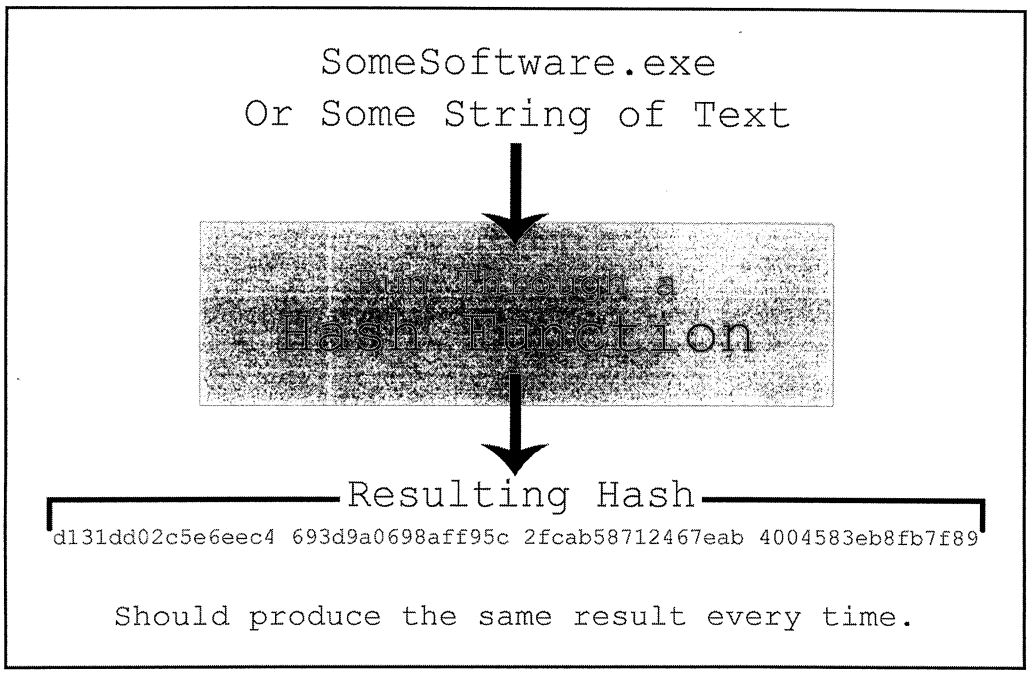
While allies of former President Donald Trump have leveled spurious charges against Dominion Voting Systems surrounding the 2020 elections, they have generally turned a blind eye to questions about Election Systems and Software, LLC (ES&S), a much larger voting machine company operating in *dozens of states*, including Texas and Arizona.

Documents obtained by *WhoWhatWhy* show that, about 40 days before the 2020 election, the federal Election Assistance Commission (EAC) quietly investigated concerns that ES&S's software installation and validation methods could have left touch-screen voting systems in up to 19 states vulnerable to the installation of malicious or otherwise unapproved software. The documents also suggest that ES&S may have initially misled election officials about this issue.

The issue had been flagged by voting machine examiners in Texas and involved something called hash-validation testing, the process for confirming that a vendor has supplied its customers with certified voting software. The examiners feared the machines could be vulnerable to manipulation and to malware. Questions remain as to whether the issue was fully resolved before the election for all affected systems in all affected states. Both the EAC and ES&S have declined *WhoWhatWhy's* requests for comment.

The documents, produced by the office of the Texas secretary of state after a public records request, show that the investigation arose from the discovery by Texas voting machine examiners that ES&S

had used an uncertified USB stick method to install software updates for some versions of its ExpressVote touchscreen voting machines. Software installed with this method *didn't match the* software certified by the EAC and failed hash-validation testing, which is conducted when new or updated software is installed. It is a mathematical algorithm that maps data generated from an installed copy, and then compares that data to the algorithm of the software certified by the EAC.



From National Institute of Standards and Technology: File verification is the process of using an algorithm for verifying the integrity of a computer file. A popular approach is to generate a hash of the copied file and comparing that to the hash of the original file. Photo credit: WhoWhatWhy

ES&S told Texas officials that the discrepancy was caused by a single benign image called "sysload.bmp." This did not reassure the Texas examiners, since they still could not distinguish between expected or benign mismatches and unexpected or malicious ones. Per Texas examiner Brian Mechler, this left the system vulnerable to an "insider threat."

On September 23, after more than a month of interoffice communications and fact gathering, Texas reported this issue to the EAC. The EAC opened an investigation which quickly expanded to include up to 18 more states and up to 35 versions of the ExpressVote. The issue and the investigation were never reported or referenced publicly.

minimal effect and said its decision was based on the advice of two voting system test labs. The lab reports show they forensically analyzed the stick method & hash mismatch for 19 versions of the ExpressVote.

But the reports, which the EAC forwarded to state officials, gave instructions for jurisdictions to distinguish between expected/benign mismatches and unexpected, possibly malicious ones. There is no indication in the documents that the EAC told state officials they were required to follow these instructions.

One reason these issues didn't become public is the EAC didn't post the "engineering change order" to their website until February 2021, around the time that *WhoWhatWhy* asked them for related documents. Initially, the website stated that the change order was approved on February 11, 2021, and that it applied to 35 ExpressVote versions, 16 more than the labs had analyzed before the election. *WhoWhatWhy* asked the EAC and ES&S about the discrepancies in the dates — October 2020 versus February 2021 — and the number of systems involved. They declined to comment, but the EAC quickly changed its website to reflect that the change order (ECO 1100) was instead granted last October and that it applied to only 19 systems.

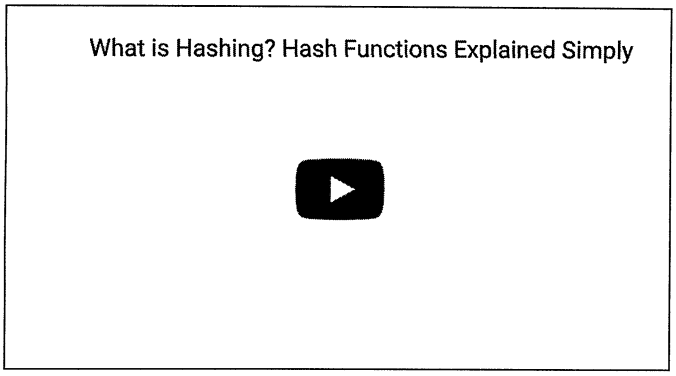
The shifting number of affected ES&S systems raises the question of whether some affected systems did not receive proper software installation and hash-validation testing before the 2020 election. At a minimum, it warrants explanation. But the EAC and ES&S have declined to comment for this story. Although *WhoWhatWhy* sent a Freedom of Information Act request to the EAC on January 11, 2021, it replied that its response will be delayed due to the pandemic.

> **"It's a gift wrapped opportunity to an insider threat, however unlikely. Under the current guidance from ES&S, an insider now knows specifically which file is not being inspected. It's similar to a bank robber knowing that the camera covering teller #3 is broken."**

Meanwhile, the documents produced by the Texas secretary of state reveal that the Texas office had additional concerns regarding ES&S's hash-validation methods. One was that ES&S's hash-verification script for election-management systems included a bug that caused it to incorrectly report a match under certain circumstances. The other was that ES&S was conducting the hash-validation tests itself, as opposed to having the jurisdictions conduct them, a "fox guarding the henhouse" situation, as one of the examiners remarked. Texas certified one of ES&S's new systems despite these concerns.

To be clear, none of these issues prove that election fraud occurred in 2020 or in prior elections. But they do suggest the EAC should publish the results of its investigation and respond substantively to questions about it, that it has not been transparent so far, and that ES&S's procedures and coding practices warrant further scrutiny. ES&S's hash-validation travails also illustrate the risks associated with using touchscreens, such as ES&S's ExpressVote, to do what most voters could easily do with a pen: mark paper ballots.

Texas discovered the issues with ES&S's hash-validation methods in the course of examining two federally certified ES&S systems: EVS 6.1.1.0 and EVS 6.0.3.0. The examinations were attended by election examiners for Texas Secretary of State Ruth R. Hughes and for Attorney General Ken Paxton. The documents given to *WhoWhatWhy* include the examiners' reports for each system and numerous interoffice communications.



Problem 1: Hash Mismatch Due to Uncertified Installation Method – Related EAC Investigation

Texas examiner Brian Mechler's report for ES&S system version EVS 6.0.3.0 stated that when the examiners asked to run the ExpressVote hash-validation process themselves on the system in August, ES&S disclosed that it had two methods for installing software updates for that version. Updates installed with its "full Inno burn" method matched ES&S's EAC-certified software and thus would pass the hash-validation test. But software installed with the faster USB stick method did not match the EAC-certified software due to what ES&S described as a single benign file called "sysload.bmp." This resulted in a hash-mismatch report, which Mechler's report called a "Hash Verification Failure." Mechler further reported, "The fact that the failure occurs on only one file is of no comfort because it still opens a vulnerability to an insider threat." Mechler's report on this issue is linked here.

In a letter to ES&S from Keith Ingram, the director of elections for the Texas secretary of state, Ingram advised that "our examiner noted that this issue could create a potential security vulnerability as a proper software validation could not occur."

In early September, ES&S representative Susan Parmer told Chuck Pinney, an attorney for the Texas secretary of state, that the voting system test lab knew about the stick-installation method and hash discrepancy when it tested EVS 6.0.2.0 and 6.0.3.0 for EAC certification and "considers it a match if this is the only file that comes up as a mismatch during verification." But she acknowledged it wasn't documented.

Mechler, in turn, sent an email to Pinney, stating that it was "troubling" that they were being "asked to take ES&S at their word" and that EAC test labs said "'this is fine.'" He expressed concern that ES&S may actually have hidden its stick-installation method and resulting hash discrepancy during the prior examination and certification of a third system.

Mechler added that "bmp files can be used to exploit systems." He also expressed concern that jurisdictions had no mechanism to verify whether hash discrepancies resulting from stick installations were due to the expected bmp file mismatch or an unexpected one:

Susan [Parmer] finishes her response by claiming, "Any other modification to that file [*the one causing* the discrepancy] would also produce a mis-match and be flagged by the export process, providing the information needed to verify the file and detect an external attack." But that is not true. There is already a mis-match and if customers are being told to ignore it, there is nothing to be flagged.

Tom Watson, another Texas examiner, agreed with Mechler's original assessment via email to the Texas secretary of state's attorney. Then Mechler came back with even stronger language:

"I think it's potentially worse than that. It's a gift wrapped opportunity to an insider threat, however unlikely. Under the current guidance from ES&S, an insider now knows specifically which file is not being inspected. It's similar to a bank robber knowing that the camera covering teller #3 is broken."

The documents indicate that by late September ES&S admitted that the stick-installation method "was not presented to the Election Assistance Commission (EAC) as part of the certification."

Moreover, a draft letter written by Executive Director Mona Harrington of the EAC, which was approved by the Texas office on September 29 and given to *WhoWhatWhy*, suggests that ES&S may have misrepresented what the the voting system test lab knew and said about this issue:

The ES&S representative performing the installation during the examination used a method that was not tested by an EAC-accredited voting system test lab (VSTL) or certified by the EAC to install the software. When questioned by the Texas SOS representatives, the representative claimed that the installation method was reviewed/approved by the lab as part of their certification. Both SLI (VSTL for EVS 6.0.2.0) and Pro V&V (VSTL for EVS 6.0.3.0) deny that they had reviewed this installation method as part of certification testing.

(The Texas office produced only the draft of this letter, not a signed copy. The EAC has yet to respond to *WhoWhatWhy's* document request submitted in January. The EAC and ES&S declined our request for comment.)

ES&S also initially misled Texas officials when it claimed that "this [hash] discrepancy did not exist on any fielded ExpressVotes since all were loaded with a full install." ES&S later acknowledged this claim was incorrect. As reported by Watson, one of the Texas examiners, "There are fielded ExpressVote machines that would fail the hash test for the incorrect sysload.bmp file."

> **"It is the ultimate 'fox watching the henhouse' scenario. It is them [ES&S] self-certifying systems for use." — Brandon Hurley**

On September 15, when Christina Adkins, the legal director for the Texas secretary of state, learned the uncertified installation method had been used in the field after all, she sent an email to Parmer of ES&S stating that, "Essentially what you've told us ... is that there are Texas customers who received software upgrades that failed the hash validation process, and that ... you did not inform our office. ... This is very concerning and *raises doubts about our ability to trust your team to report and address these issues with us.*" (italics added.)

In an email the next day, Parmer tried to persuade Adkins that the hash-mismatch "did not fail" and thus there was "never ... an issue to report," reasoning that the mismatch was caused by a single benign file and that ES&S had prior knowledge of the discrepancy and thus "expected" it. "The hash validation process ... did not fail," she wrote. "On the contrary, the software did exactly what we expected it to do when a stick update is used on an ExpressVote 1.0 and verified the SYSLOAD.BMP fil

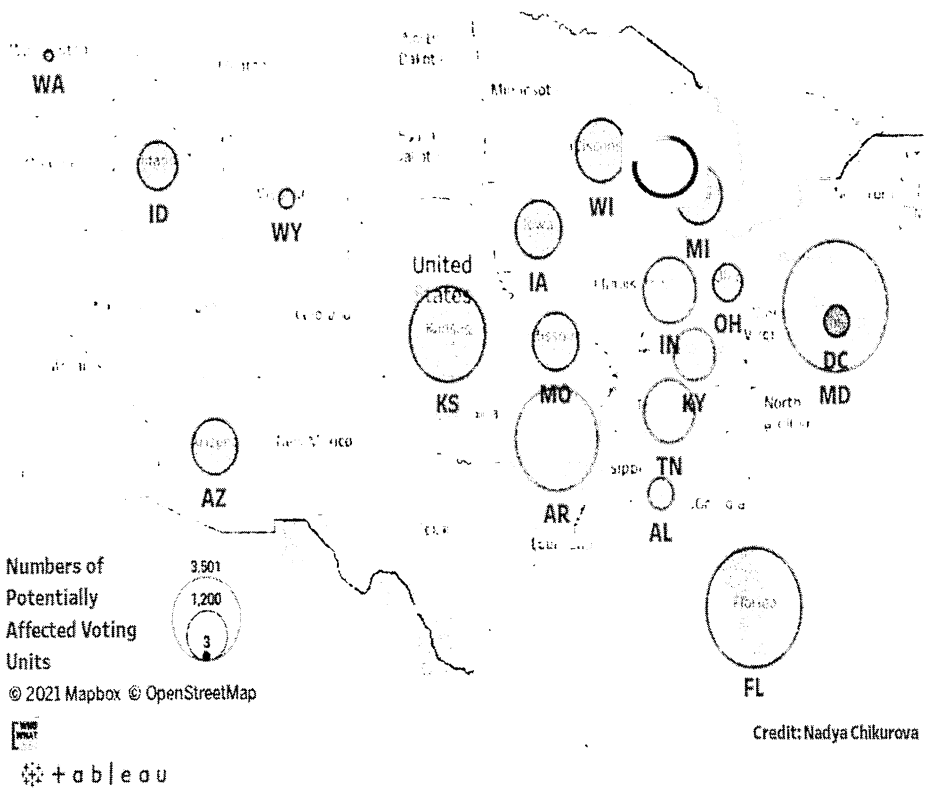
was not present. This was the expected result, and, as such, is considered a match. ... There has never been an issue to report and it is disheartening to think your team would doubt our integrity in this matter."

Adkins determined that was not acceptable:

The only thing that the jurisdiction has to go on here is your word that the mismatch is the expected result. They have no way of knowing whether the mismatch occurred because it is the expected mismatch, or because the mismatched file was somehow altered or manipulated. ... Regardless of whether ES&S considers this to be a successful hash verification and a successful match, our office does not consider the verification process to be successful under those conditions.

On October 1, Harrington of the EAC sent a letter to state election directors which stated that, "Initially, we were under the impression that only EVS 6.0.2.0 systems in Texas were impacted. We [are] requesting information from ES&S to better understand the scope and to date have received information that the states listed in Table 1 have at least one jurisdiction that may be affected."

Hash Validation Errors in ES&S machines



Credit: Nadya Chikurova

- Alabama (105 units potentially affected),
- Arkansas (2072 units potentially affected),
- Arizona (496 units potentially affected),
- Washington, DC (102 units affected),

- Florida (2893 units potentially affected),
- Iowa (532 units potentially affected),
- Idaho (346 units potentially affected),
- Indiana (731 units potentially affected),
- Kansas (1742 units potentially affected),
- Kentucky (400 units affected),
- Maryland (3501 units likely unaffected),
- Michigan (548 units potentially affected),
- Missouri (538 units potentially affected),
- Ohio (168 units potentially affected),
- Tennessee (671 units potentially affected),
- Washington (3 units potentially affected),
- Wisconsin (667 units potentially affected),
- Wyoming (20 units potentially affected).

The letter further stated that "Table 2 displays all affected EVS voting systems." Table 2, in turn, listed *35* different EVS systems.

On October 7, Harrington emailed state officials a list of talking points to help officials in case of inquiries. They stated that as a remedial measure, the EAC had asked ES&S to submit all information and affected versions for forensic testing by two EAC-approved Voting System Test Labs, SLI Compliance and Pro V&V, to see if they would qualify as a minor change.

A week later, Harrington emailed state officials again, declaring that both labs had completed all the testing ahead of schedule and approved the stick-installation method as a "de minimis" change. A few days later, she emailed them the EAC's change-order approval.

Buried at the end of the SLI lab reports, however, is an instruction for jurisdictions using the stick-installation method. The SLI reports state that in the event of a hash mismatch, "the jurisdiction must ... verify that the sysload.bmp files' hash codes ... match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S's recommendations and perform a Production Image installation on the device."

Although Harrington (EAC) forwarded the lab reports to state officials on October 15, her email stated only, "As promised, attached are the final lab reports," and said nothing about the instructions. The dav

before, she wrote that the labs had approved the "de minimis" finding, that the EAC "concurred," and that she would be "sending the reports, nothing beyond that."

Concerns regarding ES&S's previously uncertified installation method and resulting hash discrepancy were effectively buried. The EAC didn't post the change order to its website until February 2021, after *WhoWhatWhy* asked them for documents, which have yet to be provided. In Texas, the secretary of state's office extended the deadline for examiners to submit reports for the system where the issue came up until after the election and gave ES&S permission to "withdraw" its certification request for that system, which meant the reports would not be published on the secretary of state's website. The office then told the examiners that, in light of the withdrawal, the attorney general's examiners need not submit their reports to the Texas secretary of state at all, and that none of the reports had to say whether the examiners would have recommended certification.

Meanwhile, the documents produced by the Texas secretary of state show that, per their request, ES&S did a full Inno burn install on all Texas counties that it said had been impacted by the mismatch issue (stick installation). But on November 18, well after the election, Adkins wrote in an email to Mechler that she had scheduled a "meeting with ESS in December to discuss the scope of this [stick installation and hash mismatch] issue as it appears to have affected more systems than they initially disclosed to us." Mechler similarly wrote in his November 19 report that "it is unclear at this time whether there are more affected systems in Texas than initially disclosed by ES&S." Again, the Texas office declined *WhoWhatWhy's* request for comment.

An electronic ballot marker, the ExpressVote made by Election Systems & Software.
Photo credit: Douglas W. Jones / Wikimedia Commons (CC0)

Problem 2: Bug in ES&S's Hash Verification Script

Even if all hash discrepancies caused by stick installations were properly verified before the election, Texas had additional concerns with ES&S's hash-validation methods, including a bug in ES&S's hash-verification script. As explained in Mechler's report, the process required two USB thumb drives —

one with the export data being verified and one with the scripts and hash file. These need to match. Even when Mechler neglected to add the hash file for the certified version of the software, the software still reported a match. Per Mechler's report:

"While working through the [hash validation] process, I initially overlooked the instruction to add the trusted hash file to the scripting media. Despite the missing trusted hash file, the verification script erroneously reported that the exported hashes matched the trusted [certified] hashes."

This means that even though no hash comparisons were made, the verification implies a good result.

Mechler wrote, "In my opinion, this bug (in addition to the overall process) indicates that ES&S has not developed their hash verification with sufficient care, quality assurance, and concern for usability."

Problem 3: ES&S Conducting Its Own Hash-Validation Tests

In the course of email communications about the stick-installation method, Parmer of ES&S mentioned in an email to Pinney, a lawyer for the Texas secretary of state, that ES&S technicians were conducting the hash-validation tests themselves, as opposed to having the jurisdictions conduct them. This alarmed the examiners and the Texas secretary of state's office because the purpose of hash validation is to ensure the vendor hasn't given its customers something different than what was certified.

As explained in an email from Adkins, the legal director for the Texas secretary of state, to ES&S's Parmer, "If the hash validation process is performed by the same vendor technician who performed the installation, then that validation process loses one of its major purposes, which is to keep the vendor honest."

Brandon Hurley, one of the examiners for the Texas secretary of state, similarly stated in an email to Adkins and other Texas examiners that, "It is the ultimate 'fox watching the henhouse' scenario. It is them [ES&S] self-certifying systems for use."

"Jurisdictions should always perform this process themselves," Mechler wrote in his reports. "To have the vendor [ES&S] perform a required component of acceptance testing creates, at best, a conflict of interest."

But, as reported in the blog *Freedom to Tinker*, at least one ES&S contract in Texas expressly requires the customer to use ES&S for hash-validation testing. Here is the provision:

IN THE EVENT THE CUSTOMER DECLINES ES&S' INSTALLATION AND ACCEPTANCE TESTING SERVICES, OR IN ANY WAY AT ANY TIME ALTERS, MODIFIES OR CHANGES ANY EQUIPMENT, SOFTWARE, THIRD PARTY ITEMS, AND/OR NETWORK, (COLLECTIVELY "SYSTEM") CONFIGURATIONS WHICH HAVE BEEN PREVIOUSLY INSTALLED BY ES&S OR WHICH ARE OTHERWISE REQUIRED IN ACCORDANCE WITH THE CERTIFIED VOTING SYSTEM CONFIGURATION, ALL WARRANTIES OTHERWISE PROVIDED HEREUNDER WITH RESPECT TO THE SYSTEM PURCHASED, LEASED, RENTED AND/OR LICENSED UNDER THIS AGREEMENT SHALL BE VOID AND OF NO FURTHER FORCE AND EFFECT.

Eddie Perez, an election technology expert with the OSET Institute, recently called this type of contract provision "unconscionable."

Photo credit: @eddieperezTX / Twitter

It's "like buying a new home and before the closing the seller says, 'You don't need a final walk-through. Just trust me," Perez added. "And then 'voiding the warranty' if they don't agree? Unethical strong-arming at its worst."

Photo credit: @eddieperezTX / Twitter

Texas Certifies EVS 6.1.1.0 Despite Hash-Validation Concerns

The Texas Election Code states that a "voting system may not be used in an election unless the system ... is safe from fraudulent or unauthorized manipulation."

Despite the hash-validation concerns discussed in the examiners' reports, and Mechler's assertion in his report that "the hash verification process has been a growing issue of concern over the past few certification exams," Mechler and the other examiners ultimately recommended that Texas certify EVS 6.1.1.0. Texas took their advice and certified that system on January 8, 2021.

Meanwhile, Texas Attorney General Ken Paxton has expressed no concern about his state's use of ES&S systems despite having publicly assailed Dominion Voting — ES&S's main competitor — in an effort to help Donald Trump's so-called "Stop the Steal" campaign. That campaign relied, in part, on an error-riddled affidavit by discredited "expert" Russ Ramsland regarding election results produced by Dominion Voting in Michigan. But during an interview last October, it was ES&S that Ramsland accused of manipulating elections in Texas.

According to Ramsland, elected leaders in Texas weren't "paying a lot of attention to this." In 2019, Ramsland said he'd had "a couple of meetings with the [Texas] AG's office," but "one of their guys was the very guy that certified these people as being safe. So he is ... very conflicted right off the bat. He's gotta protect his reputation."

In Arizona, the GOP now wants Ramsland to forensically analyze Dominion Voting machines in Maricopa County, but has made no such demand regarding ES&S machines, which are used in other Arizona counties. According to the EAC's October 1 letter, Arizona was potentially affected by the stick-installation and hash discrepancy issues for ES&S's ExpressVote.

To be clear, *WhoWhatWhy* is aware of no evidence that systems supplied by ES&S were exploited to rig an election. But ES&S's hash-validation problems nonetheless show that ES&S does not deserve a free pass from public scrutiny and that the EAC has not been transparent about what transpired.

Touchscreen Voting Machines and the Vanishing Black Votes

According to investigative journalist and longtime election integrity blogger and broadcaster Brad Friedman, these issues also "underscore the absurdity of using expensive, complicated ... touchscreens like the ExpressVote to mark 'paper ballots' for voters who are ... capable of doing so themselves with nothing more than a simple pen." Unlike the ExpressVote, pens can't be hacked and don't require hash-validation testing to keep them honest.

"Texas requires counties to manually tabulate the votes in 1 percent of precincts (or three precincts, if greater) that have paper records," professor Philip Stark, America's preeminent election-auditing expert, told *WhoWhatWhy.* "Depending on the nature of the election, the manual count includes either 'not more than three offices and not more than three propositions' or all contests on the ballots in the selected precincts. This audit procedure cannot catch incorrect reported outcomes, even if there were a trustworthy paper trail for every vote — which is not the case."

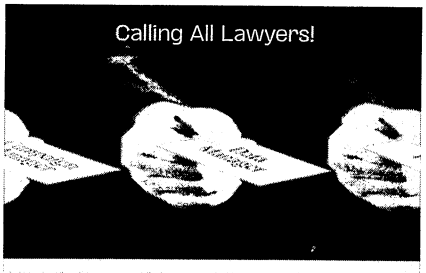
In 2019, House Democrats passed the Securing America's Federal Elections (SAFE) Act, which would have required robust manual audits called risk-limiting audits for all federal races and banned most of the current generation of touch screens, including the ExpressVote. But the GOP blocked the SAFE Act.

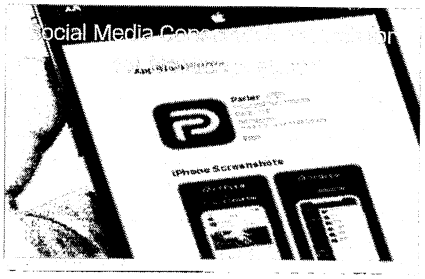
According to the National Voting Rights Task Force (in full disclosure, the writer is a member of said group), hand-marked paper ballots are preferable to touch screens for in-person voting, with an exception for voters with disabilities, because they are "quicker, safer, and inherently verified by the voter in the act of marking. Maintaining the integrity of in-person voting is crucial in light of the attacks on vote by mail." It remains to be seen whether the new Congress will heed this advice.

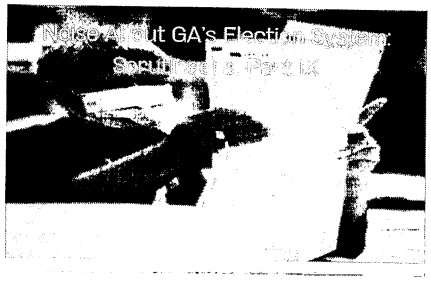
For more of WhoWhatWhy*'s work on Protecting Our Vote, see our Student Voter Guide and our series America Decides 2020. You can also find out the darker secrets behind our voting systems in our recently published e-book* Is This Any Way to Vote?: Vulnerable Voting Machines and the Mysterious Industry Behind Them *by Celeste Katz Marston and Gabriella Novello, available on Amazon now.*

Related front page panorama photo credit: Adapted by WhoWhatWhy from Wikipedia and ES&S / Wikimedia.

Related Posts:







Comments are closed.

Subscribe to the Daily WhoWhatWhy

Relevant, in-depth journalism delivered to you.

Email *(Required)*

Name *(Required)*

First

Last

SIGNUP

From: Christina Adkins
To: Brian Mechler
Cc: [redacted]; [redacted]; [redacted] Lesley.French@oag.texas.gov; [redacted] Austin.Kinghorn@oag.texas.gov; Charles Pinney
Subject: Re: EVS 6030
Date: Thursday, November 19, 2020 12:45:46 PM
Attachments: image001.png

My understanding is that they are seeking it for all affected versions. I think it just needs to work it's way through the process administratively. I can reach out to the EAC to confirm.

And before you ask, we have a meeting with ESS in December to discuss the scope of this issue as it appears to have affected more systems than they initially disclosed to us.

From: Brian Mechler [redacted]>
Sent: Thursday, November 19, 2020 12:32:37 PM
To: Christina Adkins <CAdkins@sos.texas.gov>
Cc: [redacted]>; [redacted]>; Lesley.French@oag.texas.gov <Lesley.French@oag.texas.gov>; [redacted]; Austin.Kinghorn@oag.texas.gov <Austin.Kinghorn@oag.texas.gov>; Charles Pinney <CPinney@sos.texas.gov>
Subject: Re: EVS 6030

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Just in case anyone was worried or curious, the SYSLOAD.BMP file that failed the EVS 6.0.3.0 hash verification process does match with one of the previous FW versions, 1.4.1.2

I can't find anything on the ECO on the EAC website yet. The Pro V&V report lists a whole slew of affected versions, but the SLI report only identifies 6.0.3.0 as affected. Do we know for which versions ES&S is seeking EAC approval of the ECO?

Brian

On Wed, Nov 18, 2020 at 11:15 AM Christina Adkins <CAdkins@sos.texas.gov> wrote:

> Dear Examiners:

From: Keith Ingram
To: Christina Adkins; Charles Pinney
Cc: Adam Bitter
Subject: FW: Notification to States- ES&S- Lab report
Date: Thursday, October 15, 2020 11:48:21 AM
Attachments: ES&S ECO 1100 - SLI Analysis.zip
ES&S ECO 1100 - Pro V&V Analysis.zip

From: Mona Harrington <mharrington@eac.gov>
Sent: Thursday, October 15, 2020 11:35 AM
To: [redacted]; kea.warne@state.sd.us; linda.lamone@maryland.gov; meagan.wolfe@wisconsin.gov; ssandvoss@elections.il.gov; kai.schon@wyo.gov; chris.piper@elections.virginia.gov; bking@iec.in.gov; bdul@azsos.gov; braterj@michigan.gov; Keith Ingram <KIngram@sos.texas.gov>; Anthony.Albence@delaware.gov; Apmiller@dcboe.org; mark.goins@tn.gov; 'Michael' <micmoser@pa.gov>; agrandjean@ohiosecretaryofstate.gov; jared.dearing@ky.gov; bryan.caskey@sos.ks.gov; wthorley@sos.nv.gov; 'Lori Augino' <lori.augino@sos.wa.gov>; Maria.Matthews@DOS.myflorida.com; kendra.lane@sos.mo.gov; clay.helms@sos.alabama.gov; heidi.burhans@sos.iowa.gov; hawley.robertson@sos.ms.gov; leslie.bellamy@sos.arkansas.gov; jason.hancock@sos.idaho.gov; [redacted]
Cc: Kevin Rayburn <KRayburn@eac.gov>; Jerome Lovato <jlovato@eac.gov>
Subject: RE: Notification to States- ES&S- Lab report

[redacted]

Good afternoon everyone,
I hope this email finds you all well. As promised attached are the final lab reports.
Best,
Mona

From: Mona Harrington <mharrington@eac.gov>
Sent: Wednesday, October 14, 2020 2:55 PM
To: [redacted] kea.warne@state.sd.us; linda.lamone@maryland.gov; meagan.wolfe@wisconsin.gov; ssandvoss@elections.il.gov; kai.schon@wyo.gov; chris.piper@elections.virginia.gov; bking@iec.in.gov; bdul@azsos.gov; braterj@michigan.gov; kingram@sos.texas.gov; Anthony.Albence@delaware.gov; Apmiller@dcboe.org; mark.goins@tn.gov; 'Michael' <micmoser@pa.gov>; agrandjean@ohiosecretaryofstate.gov; jared.dearing@ky.gov; bryan.caskey@sos.ks.gov; wthorley@sos.nv.gov; 'Lori Augino' <lori.augino@sos.wa.gov>; Maria.Matthews@DOS.myflorida.com; kendra.lane@sos.mo.gov; clay.helms@sos.alabama.gov; heidi.burhans@sos.iowa.gov; hawley.robertson@sos.ms.gov; leslie.bellamy@sos.arkansas.gov; jason.hancock@sos.idaho.gov; [redacted]
Cc: Kevin Rayburn <KRayburn@eac.gov>; Jerome Lovato <jlovato@eac.gov>
Subject: Re: Notification to States- ES&S- Lab report
Hi Amy, We concurred with their findings that supported approving the requested de minimus change. That means we are not challenging their findings and are satisfied with the work performed. I will be sending the reports, nothing beyond that. I hope that helps.
Get Outlook for iOS

From: Tom Watson
To: Brian Mechler
Cc: Charles Pinney; [redacted]; French, Lesley; Cheryl Sneeringer; austin.kinghorn@oag.texas.gov; Christina Adkins
Subject: Re: Vendor Responses to Examiner Questions - EVS 6030 and 6110
Date: Friday, September 4, 2020 1:58:47 PM

Agreed. We should always consider the insider threat.

Tom

On Fri, Sep 4, 2020 at 1:47 PM Brian Mechler <[redacted]> wrote:

> I think it's potentially worse than that. It's a gift wrapped opportunity to an insider threat, however unlikely. I harp on the hash verification process because an insider with sufficient knowledge and physical access can do bad things to systems. How do we thwart that? Through good procedures, one of which is checking that what is installed on the system matches exactly with what was certified by the EAC. Under the current guidance from ES&S, an insider now knows specifically which file is not being inspected. It's similar to a bank robber knowing that the camera covering teller #3 is broken.
>
> It sounds like this was also an issue with the stick upgrade process for 6.0.2.0. Was the SoS ever notified?
>
> Brian
>
> On Fri, Sep 4, 2020 at 12:35 PM Tom Watson <[redacted]> wrote:
>
> > Chuck,
> >
> > I agree with Brian. If the customer is instructed that there is a discrepancy in a hash, they might be inclined to ignore any mis-match. Not sure what the easiest remedy is. We don't want jurisdictions ignoring the hash checks for this release or future releases.
> >
> > Tom
> >
> > On Thu, Sep 3, 2020 at 6:08 PM Brian Mechler [redacted]> wrote:
> >
> > > Chuck,
> > >
> > > The response from ES&S is troubling. There is no paper trail documenting the exception the VSTL made for this breakdown in the hash verification process nor was written documentation provided to or prepared for customers. We are being asked to take ES&S at their word that the VSTL said "this is fine." We are also being asked to take ES&S at their word that they provided appropriate guidance to their customers. This issue apparently also exists for 6.0.2.0, yet it does not appear in any of the examiners' reports. Either this issue was not disclosed or exposed during that exam or there is some nuance that I fail to understand.
> > >
> > > Susan finishes her response by claiming, "Any other modification to that file would also produce a mis-match and be flagged by the export process, providing the information needed to verify the file and detect an external attack." But that is not true. There is already a mis-match and if customers are being told to ignore it, there is nothing to be flagged.
> > >
> > > Can the State of Texas mandate that all upgrades be performed using the full iono install method?
> > >
> > > Brian
> > >
> > > On Thu, Sep 3, 2020 at 9:09 AM Charles Pinney <CPinney@sos.texas.gov> wrote:
> > >
> > > > Brian,

From: Christina Adkins
To: Keith Ingram; "Mona Harrington"
Subject: RE: ESS ExpressVote 1.0 Trusted Build Response
Date: Tuesday, September 29, 2020 3:57:00 PM

I agree with Keith.

From: Keith Ingram <KIngram@sos.texas.gov>
Sent: Tuesday, September 29, 2020 3:54 PM
To: 'Mona Harrington' <mharrington@eac.gov>
Cc: Christina Adkins <CAdkins@sos.texas.gov>
Subject: RE: ESS ExpressVote 1.0 Trusted Build Response

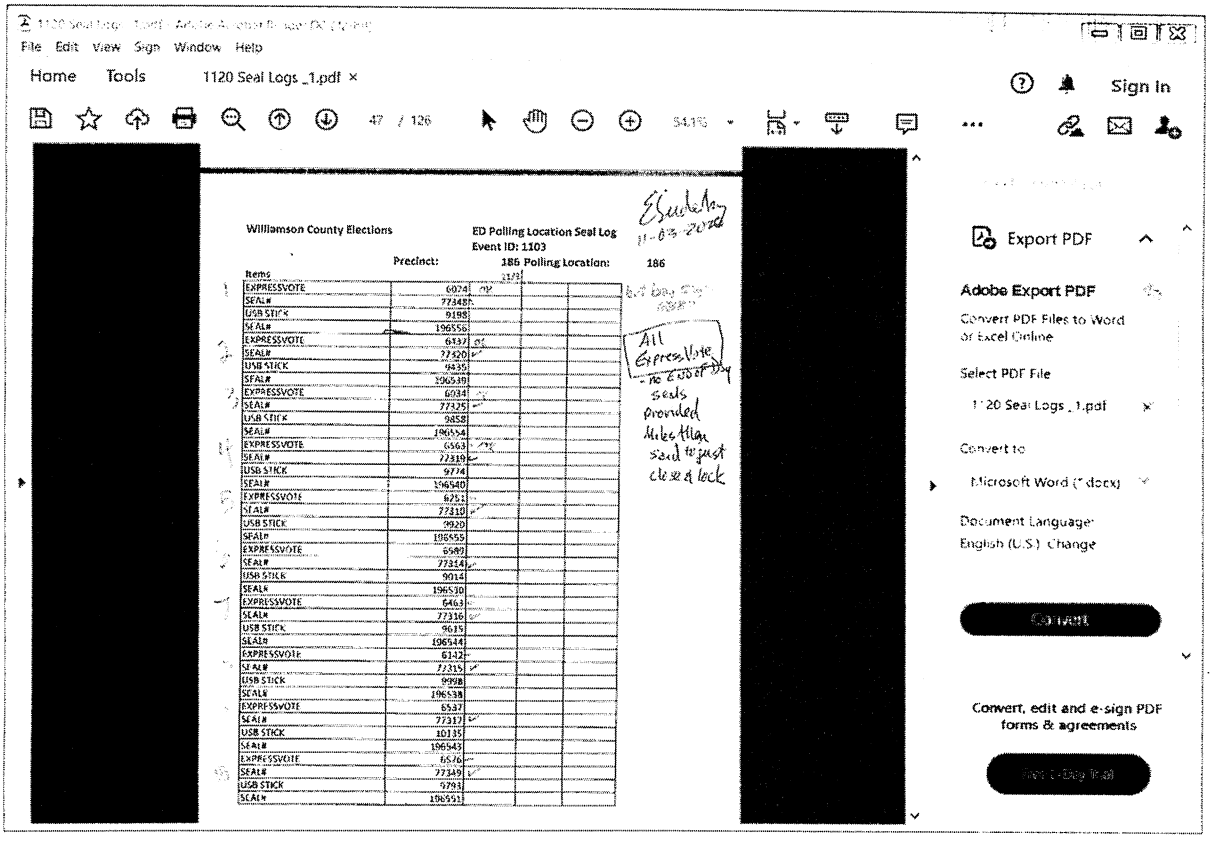
This looks fine to me. Christina is headed down to read it.

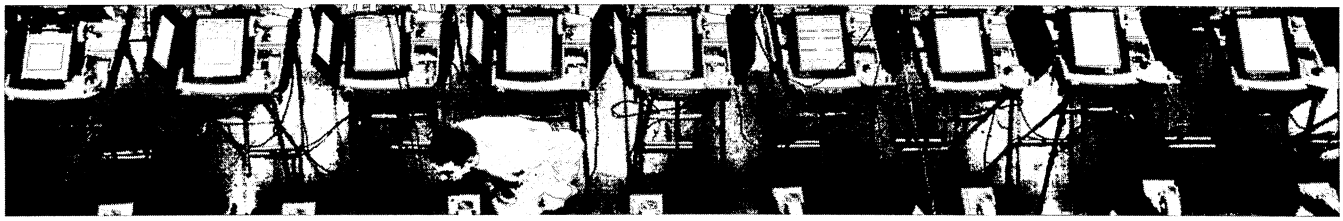
From: Mona Harrington <mharrington@eac.gov>
Sent: Tuesday, September 29, 2020 3:53 PM
To: Keith Ingram <KIngram@sos.texas.gov>
Cc: Christina Adkins <CAdkins@sos.texas.gov>
Subject: ESS ExpressVote 1.0 Trusted Build Response

Please review for accuracy as we mention Texas in numerous places.

May I also please get the correspondence between ES&S and Texas.

Thank you,
Mona Harrington


File Edit View Sign Window Help
Home Tools
1120 Seal Logs _1.pdf
47 / 126
Sign In
Williamson County Elections
ED Polling Location Seal Log
Event ID: 1103
Precinct:
186 Polling Location:
186
Items
EXPRESSVOTE 6024
SEAL# 77348
USB STICK 9198
SEAL# 196556
EXPRESSVOTE 6437
SEAL# 77320
USB STICK 9435
SEAL# 196539
EXPRESSVOTE 6034
SEAL# 77325
USB STICK 9458
SEAL# 196554
EXPRESSVOTE 6563
SEAL# 77319
USB STICK 9774
SEAL# 196540
EXPRESSVOTE 6251
SEAL# 77310
USB STICK 9929
SEAL# 196555
EXPRESSVOTE 6589
SEAL# 77314
USB STICK 9014
SEAL# 196530
EXPRESSVOTE 6463
SEAL# 77316
USB STICK 9635
SEAL# 196544
EXPRESSVOTE 6142
SEAL# 77315
USB STICK 9908
SEAL# 196538
EXPRESSVOTE 6537
SEAL# 77317
USB STICK 10135
SEAL# 196543
EXPRESSVOTE 6576
SEAL# 77349
USB STICK 9793
SEAL# 196551
All ExpressVote
seals
provided
Mike Allen
said to just
close & lock
Export PDF
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
1120 Seal Logs _1.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert, edit and e-sign PDF forms & agreements



These Diebold touchscreen voting machines, being inspected here back in 2013, are still in use in Shelby County, TN. Photo credit: © Jim Weber/The Commercial Appeal/ZUMAPRESS.com

ELECTIONS

Touchscreen Voting Machines and the Vanishing Black Votes

JENNIFER COHN @JENNYCOHN1 05/27/20

Protecting Our Vote 2020

Votes from predominantly black precincts have mysteriously vanished from touchscreen voting machines in both Tennessee and Georgia in recent elections. Georgia replaced the touchscreen system it had been using since 2002 with yet another controversial touchscreen system, rejecting the advice of most election security experts, who note that hand-marked paper ballots are less vulnerable to both tampering and error. A political battle is now raging in Shelby County — Tennessee's most populous county — over whether it will follow in Georgia's footsteps or switch to hand-marked paper ballots for the general election in November.

Shelby County is approximately 54 percent African American, a demographic that has traditionally overwhelmingly favored Democrats. But the county election commission is led by Republicans, due, in part, to state law that gives control to the party that controls the state legislature.

The loss of black votes from touchscreen voting machines in Shelby County was discovered by election commissioner Bennie Smith, a Democrat, in 2015. The debate over a new voting system

has led to a knock-down, drag-out fight, pitting Smith and election security reformers against Republican election administrator Linda Phillips and other election commissioners (three Republicans and one Democrat) who recently voted to buy controversial new touchscreen voting machines called "ballot-marking devices" (BMDs) for use by most voters at the polls. Before the vote, Republicans in the Tennessee legislature wrote a letter to the Republican election commissioners, advising that they wanted them to replace the existing touchscreen system with more touchscreens (BMDs) rather than hand-marked paper ballots.

A BMD functions as an electronic ballpoint pen and marks the ballot for the voter. A separate or integrated scanner does the actual counting. Nearly all of the current generation of BMDs, including those chosen by Shelby County, record votes on paper with a barcode, which is impossible for the voter to read. In most cases, voters cannot decipher the barcodes with a smartphone, because the barcodes are proprietary to the vendor.

Richard DeMillo, an election security expert and a computer science professor at the Georgia Institute of Technology, warns that the barcode represents a new potential target for hackers since it can be altered to flip votes.

Photo credit: Fred the Oyster / Wikimedia

BMDs print a readable text beneath the barcode on the paper, but that text is not counted by the scanner, which instead counts the votes hidden in the barcodes. As explained by election security experts, a postelection audit comparing a manual total of the votes shown in the text to the reported electronic total can reveal problems with the ballot-counting machines (scanners), but cannot reveal whether the BMDs marked the text correctly. It's up to individual voters to notice whether the BMD accurately represented their intention.

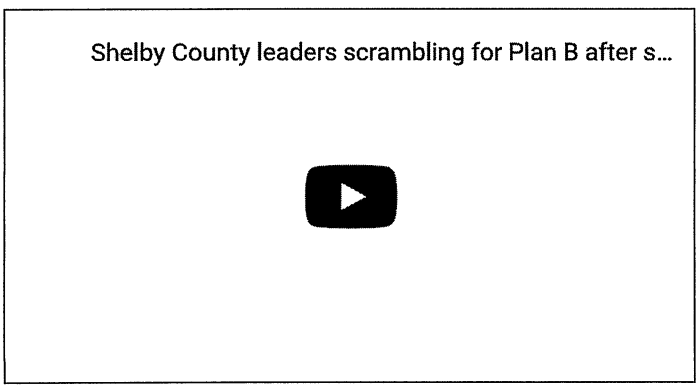
As indicated in a recent study co-authored by J. Alex Halderman, an election security expert at the University of Michigan, voters reported only 7 percent of errors made by BMDs. According to

Halderman, "the implication of our study is that it's extremely unsafe [to use BMDs], especially in close elections."

Although not confirmed by the Shelby County Election Commission, local media reports state that Election Systems and Software (ES&S) will provide the county's new BMDs. Election integrity advocates had predicted that the commission would choose ES&S, not only because ES&S maintains the county's current system, but also because the company's lobbyist, MNA Government Relations, shares an office with the commission's attorney, John Ryder (who claimed during a recent meeting that his office is merely a "tenant" of MNA, that he has not discussed the "purchasing process" with MNA, and that he is not involved in that process). They also note that since 2013, ES&S has donated more than $30,000 to the Republican State Leadership Committee, whose members include Tennessee Secretary of State Tre Hargett.

Election Machines Had a Suspicious History

ES&S's corporate history does not breed confidence that election integrity will improve. In 2000, the founder of ES&S, Bob Urosevich, was named president of Global Election Systems, which later changed its name to Diebold Election Systems and sold Shelby County its current touchscreen voting machines, the ones that lost black votes. As of September 2000, Global's senior programmer, senior vice president, and largest shareholder was Jeffrey Dean, who had been convicted and served time for 23 counts of embezzlement involving sophisticated computer tampering. (Dean's criminal record was exposed by Bev Harris in her book *Black Box Voting: Ballot Tampering in the 21st Century.*)



In 2002, Diebold Inc., an ATM manufacturer, bought Global Election Systems, rebranded it as Diebold Election Systems (DES), and chose Urosevich as its president. Diebold Inc. told the Associated Press that Dean was not affiliated with DES (formerly Global), but internal memos obtained by Harris showed that DES had kept him on as a consultant after the acquisition, and that he was called back for help on at least one occasion.

Diebold CEO Walden O'Dell was a prominent supporter of George W. Bush. In 2003, he attracted notoriety by sending a letter to potential donors stating, "I am committed to helping Ohio deliver its electoral votes to the president [Bush] ... [in 2004]."

Shelby County purchased its machines from DES in 2006, just two years after the Department of Homeland Security had issued a "Cyber Bulletin" warning that Global/Diebold's central computer, which aggregated precinct totals, was vulnerable to remote hacking. The website BradBlog.com reported the alert, which was otherwise largely ignored. A lawsuit filed several years later revealed that Shelby County's computer did, in fact, contain remote-access software.

In 2009, ES&S bought DES. A year later, the antitrust division of the Department of Justice forced ES&S to sell some of DES's assets, charging that the merger accounted for 70 percent of the market in US election equipment. The assets went to Dominion Voting, which conducts some of its programming in Serbia. ES&S, nevertheless, retained a number of DES servicing and maintenance contracts, including the one for voting machines in Shelby County as well as for the state of Georgia (until last year, when Georgia bought new BMDs from Dominion).

Together, ES&S and Dominion, by 2017, controlled more than 80 percent of the US election market.

In 2018, ES&S received negative press due to the revelation that it had sold election management systems (which aggregate a county or state's precinct totals) containing remote-access software from 2000 to 2006. ES&S had previously denied selling systems with remote-access software. It now claims to have confirmed that the software was removed, but has not said how it confirmed this, whether it was removed from DES systems too, or whether it was removed before or after the 2016 election.

ES&S has also received negative media attention due to recent revelations that many of its popular precinct ballot scanners — used to count both BMD printouts and hand-marked paper ballots — have been sold with cellular modems, which send unofficial vote totals over the internet. Some of the systems on the receiving end of these transmissions have been left exposed on the internet for months and possibly years.

Consistent Voting Irregularities in Shelby County

In 2019, Bennie Smith gave a presentation during a national election integrity conference about Shelby County's alarming history of election results. According to legal papers, for example, Republicans in Shelby swept the countywide elections in August 2010 after poll workers turned 5,400 voters away during the designated early voting period because ES&S check-in computers (electronic poll books) inaccurately reported that they had already voted. The problem allegedly occurred because the wrong database had been mistakenly inserted into the computers. Smith told *WhoWhatWhy* that the error disproportionately impacted Democrats because more Democrats than Republicans tend to vote early in Shelby County.

A month later, Bev Harris examined the voting records provided by county officials for that election and found 3,221 more votes than voters. Harris noted in an article published by the *Columbus Free Press* that most of the voterless ballots came from precincts with a heavy Republican presence. The distribution was anything but random. The inspection team obtained the documents after ten defeated candidates filed a lawsuit charging election irregularities. ES&S had the Shelby County voting machine contract at that time.

Shelby County's election irregularities did not stop there. In 2012, election volunteers and city officials reported that 3,000 voters had been given the wrong ballots. Some voters had been turned away from the polls over challenges concerning their addresses. Others had simply given up when waiting periods were too long.

After an investigation, the state comptroller charged the Republican election commissioner, Richard Holden, as well as the county election board, with "poor judgment." The FBI initiated an inquiry, but then dropped the case.

In August 2014, Republicans again swept nearly all the countywide elections. Nine defeated candidates filed a lawsuit charging that Diebold's record was tainted by hackers who had conspired with the winning candidates and the election board. The case was thrown out.

In 2015, when Bennie Smith discovered the disappearance of votes from predominantly African American precincts, he documented the evidence by photographing the totals reported in poll tapes, the paper printouts generated by each machine after the polls close. He then compared the figures from the machines to the totals generated by the central computer, which revealed that votes from predominantly black precincts had been eliminated. After calls for both an investigation and the firing of Richard Holden, Holden resigned and was replaced by Linda Phillips — also a Republican.

Poll tape, Shelby County, TN, 2015. Photo credit: Courtesy Bennie Smith

In 2018, the Coalition for Good Governance (CGG), a nonprofit group in Georgia, decided to cross-reference poll tapes from Georgia precincts, which also used Diebold/ES&S touchscreen voting machines. It discovered that some 127,000 votes from predominantly black precincts had mysteriously vanished. The CGG filed a lawsuit, but the court later dismissed it because the Republican margin of victory was larger than the number of missing votes. In 2019, an election security panel hosted by Lulu Friesdat of SMART Elections discussed the alarming coincidence of ES&S/Diebold voting machines losing votes from predominantly black areas in both Georgia and Tennessee.

New Voting Vulnerabilities: Ballot-Marking Devices and Electronic Poll Books

Concerns with BMDs extend beyond unverifiable barcodes and auditability. Unlike hand-marked paper ballots, BMDs must be activated. Some jurisdictions accomplish this with "activation cards" prepared on electronic poll books — tablet computers that also confirm that people who check in to vote are properly registered and have not already voted. On the issue of BMD activation, ES&S's product overview explains that a stand-alone application called ExpressLink interfaces with the electronic poll book system and a card printer to print out an activation card that the voter then inserts into the BMD to retrieve the authorized ballot.

Using electronic poll books to activate BMDs can be risky. Duncan Buell, an election security expert who serves on the faculty of the University of South Carolina, told *WhoWhatWhy* that "in some jurisdictions the e-poll books are connected via the internet back to home base at county

headquarters. If that is the case, then one has to assume that the e-poll book is hackable and thus that the barcode is also hackable in any number of different ways." According to Buell,

"[a] more subtle danger exists if the e-poll books are connected locally, allegedly only inside a polling place, to themselves and perhaps to printers (via wifi, bluetooth, or such). Again, the danger of hacking exists, and the problem becomes much more local and thus much harder to detect."

DeMillo said that, to his knowledge, no one has studied the effect of inserting an activation card containing malware or other improper information (such as the voter's party affiliation) into a BMD, which raises a number of unanswered questions about the security of the system.

Even without malware or improper hidden information, a defective activation card can cause problems. In 2016, thirty defective smart cards in Shelby County made it "impossible to pull up the correct electronic ballot on voting machines."

Electronic poll books (e-poll books) contain voter registration lists so poll workers can check voters in quicker, and hackers exploited its cybersecurity flaws at DEF CON 27's Voting Village. Photo credit: Adapted by WhoWhatWhy from guilaine / Pixabay

There are additional concerns. If BMDs depend on electronic poll books for activation, then a connectivity issue or distributed denial of service (DDoS) attack involving the electronic poll books can prevent the use of BMDs. In a test run conducted in Georgia in January, electronic poll books from a company called Knowink failed in four out of six counties, preventing activation of the BMDs. In Indiana, ES&S electronic poll books failed due to connectivity issues in five out of seven of the counties that used them; one county clerk called it the worst election she's ever experienced in her eight years on the job. Similarly catastrophic connectivity issues with Knowink e-poll books wreaked havoc in Los Angeles County, CA, during its recent primary.

In addition, the BMDs themselves can fail. During a recent Shelby County Election Commission hearing, Richard Garella, a Pennsylvania advocate for election integrity, read a long list of six hundred complaints from poll workers regarding Philadelphia's new $29 million ES&S BMDs. These ranged from paper jams to screen freezes, machines not powering on, system lags, calibration issues, card errors, and machines spitting out and not reading ballots.

Brand-new BMD machines have failed during other recent election rollouts. In Richland County, SC, every fifth or sixth machine had problems. In Northampton County, PA, at least a third of ES&S's BMDs were miscalibrated. And in Los Angeles County, CA, 20 percent of recently acquired, custom-made BMDs crashed. The Associated Press reported that, based on state certification documents in Pennsylvania, even when ES&S BMDs don't crash, it takes the average voter three times as long to cast a vote using the BMD as it does with hand-marked paper ballots and scanners. As with all touchscreens, BMDs also limit the number of people who can vote at the same time, which leads to bottlenecks and long lines.

NAACP Sues Tennessee County Over Mismanaging Voter Registrations

Early Voting in Tennessee Hits Road Bumps Amid Registration Controversy

A blue county in Tennessee botches day one of early voting in Memphis. Reports of long lines, equipment failures, and great frustration accumulated — just days after a voter registration organization filed a lawsuit against the local election commission.

WhoWhatWhy

Compatibility Concerns With Other Equipment

Phillips hasn't said whether the new ES&S BMDs will require the replacement of other recent election equipment purchases, which are themselves the subject of controversy due to apparent conflicts of interest involving Phillps and her family. In August of 2017, the county bought a new voter registration system from a company called Everyone Counts, which employed Phillips before she took the Shelby County job.

At least one of her sons worked for Everyone Counts when the contract was made. The county already had ES&S poll books, but in 2018 it bought new ones from Knowink — whose managing director is a former Republican election official from Missouri — after Phillips advised that only

Knowink's poll books would work with the new voter registration system. But Shelby County's current Request for Proposal states that the county intends to replace its ES&S electronic poll books with new ones after it chooses new voting machines — which is curious given that it already bought new poll books from Knowink, where one of Phillips's sons now works.

On the issue of compatibility, Knowink's website lists voting-machine vendors with whom it typically partners. ES&S isn't among them. And the city of Philadelphia recently had to shelve Knowink electronic poll books after the machines failed to connect to ES&S's printers and proved inadequate when it came to election night reporting.

Bennie Smith has tried to steer Phillips and the election commissioners toward paper ballots marked by hand. Many security experts and election security advocates — such as Free Speech for People, Audit USA, NVRTF, CGC, SMARTelections, Scrutineers, and Citizens for Better Elections — recommend that approach. In contrast to BMDs, hand-marked paper ballots do not require activation from check-in computers and do not have compatibility issues. They don't risk failing because of computer malware, and they can't be improperly calibrated or programmed badly. They don't break down or cause bottlenecks that lengthen lines, and they don't conceal votes behind barcodes.

Shelby County Election Commissioner Bennie Smith (left) and Shelby County Election Administrator Linda Phillips (right). Photo credit: Courtesy of Bennie Smith and Shelby County

Moreover, a study by the University of Pittsburgh and Citizens for Better Elections found that ES&S BMDs in Pennsylvania cost almost twice as much as hand-marked paper ballots. And, according to a written analysis by the OSET Institute on election technology acquisition in Georgia, BMDs cost almost twice as much as hand-marked paper ballots over a ten-year period.

Even so, Linda Phillips and the other election commissioners voted for BMDs. Contrary to OSET's analysis, Phillips claimed that BMDs will cost less than hand-marked paper ballots in the long run.

Despite vanishing votes in Shelby County and Georgia and frequent media reports of human error causing touchscreens to flip votes, Phillips alleges without data that people make more mistakes with ballpoint pens. She claims that, according to a study she conducted of absentee ballots, voters from certain zip codes made more mistakes than voters from other zip codes when using pens. But in response to an Open Records Request for the absentee ballots used in the study, Phillips advised that "the 1088 absentee ballots ... were removed from our files as part of the routine destruction of documents. We are required to keep election materials for 22 months; then they may be destroyed. These materials do not exist."

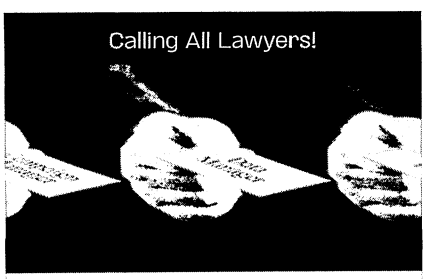
In any case, it is questionable whether a study examining absentee ballots is relevant to the use of paper ballots in a polling place where scanners can alert voters to over- and undervotes. During an election recount in Minnesota in 2008, a bipartisan panel found a total of only 14 out of 2.9 million hand-marked ballots in which the voter's intention was not clear.

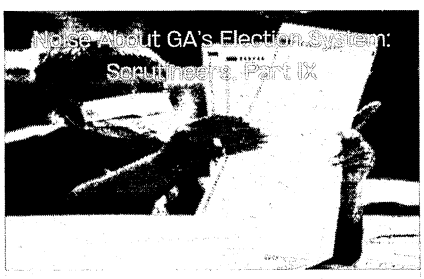
In contrast, it is common to see reports of vote-flipping touchscreens. Many voters are unlikely to notice the problem. Unless the vote is caught on camera, voters can't prove that the voting machine is responsible for the problem. Election officials and vendors often blame the problem on voter error, as occurred in 2018 in Georgia and Texas. Even when a vendor admits that its employees or others incorrectly calibrated the machines, as ES&S acknowledged with BMDs that malfunctioned in Pennsylvania's Northampton County, there is usually no remedy and no way to know whether the problem was accidental or malicious, since the software is proprietary to the vendor.

Despite the Shelby County Election Commission's vote in favor of BMDs, the battle over the county's voting machines is not over. While Republicans control the election commission, Democrats control the County Commission, which favors hand-marked paper ballots and controls the purse strings.

Related front page panorama photo credit: Adapted by WhoWhatWhy from Alexrk / Wikimedia (CC BY 3.0).

Related Posts:





5

Article Rating

3 COMMENTS

Newest

Dave 1 year ago

Sounds like the folks who cry wolf all the time are wolves themselves as their projection seems obvious to this observer.

+ 0 —

Jonathan Simon 1 year ago

This is superb, in-depth investigation, analysis, and reporting. What I hope does not get lost in the sauce is the unidirectional nature of all these "errors" and mistabulations.

I have worked in election forensics for the entire post-HAVA computerized voting era in the U.S. and, while my approach is process-oriented and nonpartisan, there is NOTHING nonpartisan about the patterns of anomaly and disparity we keep uncovering. Virtually every supposed "error" or "glitch" favors the Republican candidate – or the candidate/position that would be favored by the American far-right. That is not how errors and glitches work – they'd break 50-50, or close to it.

So these vote adds, vote losses, and vote shifts are the product of malfeasance not error, a design not a bug. Call it meddling, interference, rigging, whatever you please: the vulnerabilities to fraud of our concealed, computerized voting and vote counting processes are being exploited for political advantage, and the results should be obvious to anyone who studies ordinary and distorted political dynamics.

+ 0 —

Secure Our Vote 1 year ago

Elections are the cornerstone of our democracy, we should be taking swift action to ensure America has safe & secure elections.

If you agree, join us in the battle for safe & secure elections. We send out updates on important election security news and give you the information you need to be an election security advocate.

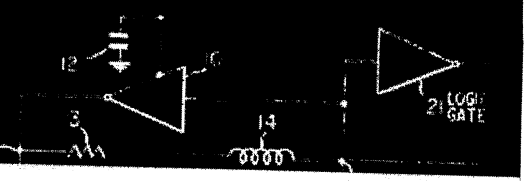
Receive updates from the Secure Our Vote campaign about steps you can take to protect our voting and registration systems,

information about training calls, and updates on election security in the news.

+ 0 −

FREEDOM TO TINKER

research and expert commentary on digital technologies in public life



Voting Machine Hashcode Testing: Unsurprisingly insecure, and surprisingly insecure

MARCH 5, 2021 BY ANDREW APPEL

By Andrew Appel and Susan Greenhalgh

The accuracy of a voting machine is dependent on the software that runs it. If that software is corrupted or hacked, it can misreport the votes. There is a common assumption that we can check the legitimacy of the software that is installed by checking a "hash code" and comparing it to the hash code of the authorized software. In practice the scheme is supposed to work like this: Software provided by the voting-machine vendor examines all the installed software in the voting machine, to make sure it's the right stuff.

There are some flaws in this concept: it's hard to find "all the installed software in the voting machine," because modern computers have **many layers *underneath* what you examine**. But mainly, if a hacker can corrupt the vote-tallying software, perhaps they can corrupt the hash-generating function as well, so that whenever you ask the checker "does the voting machine have the right software installed," it will say, "Yes, boss." Or, if the hasher is designed not to say "yes" or "no," but to report the hash of what's installed, it can simply report the hash of what's *supposed* to be there, not what's *actually* there. For that reason, election security experts never put much reliance in this hash-code idea; instead they insist that you can't fully trust what software is installed, so you must achieve election integrity by doing recounts or risk-limiting audits of the paper ballots.

But you might have thought that the hash-code could at least help protect against accidental, nonmalicious errors in configuration. You would be wrong. It turns out that **ES&S** has bugs in their hash-code checker: **if the "reference hashcode" is completely missing, then it'll say "yes, boss, everything is fine" instead of reporting an error.** It's simultaneously ***shocking*** and ***unsurprising*** that ES&S's hashcode checker could contain such a blunder ***and*** that it would go unnoticed by the U.S. Election Assistance Commission's federal certification process. It's unsurprising because testing naturally tends to focus on "does the system work right when used as intended?" Using the system in unintended ways (which is what hackers would do) is not something anyone will notice.

Until somebody ***does*** notice. In this case, it was the State of Texas's voting-machine examiner, Brian Mechler. In **his report dated September 2020** he found this bug in the hash-checking script supplied with the ES&S EVS 6.1.1.0 election system (for the ExpressVote touch-screen BMD, the DS200 in-precinct optical scanner, the DS450 and DS850 high-speed optical scanners, and other related voting machines). (Read Section 7.2 of **Mr. Mechler's report** for details).

We can't know whether that bug was intentional or not. Either way, it's certainly convenient for ES&S, because it's one less hassle when installing firmware upgrades. (Of course, it's one less hassle for potential hackers, too.)

Another gem in Mr. Mechler's report is in Section 7.1, in which he reveals that *acceptance testing* of voting systems is done by the *vendor,* not by the customer. Acceptance testing is the process by which a customer checks a delivered product to make sure it satisfies requirements. To have the vendor do acceptance testing pretty much defeats the purpose.

When the Texas Secretary of State learned that their vendor was doing the acceptance testing themselves, the SoS's Election Division took an action "to work with ES&S and their Texas customers to better define their roles and responsibilities with respect to acceptance testing," according to the report. They may encounter a problem, though: the ES&S sales contract specifies that ES&S must perform the acceptance testing, or they **will void your warranty (see clause 7b)** .

There's another item in Mr. Mechler's report, Section 7.3. The U.S. Election Assistance Commission requires that "**The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the [National Software Reference Library] or from a State designated repository. The process used to verify software should be possible to perform without using software installed on the voting system.**" This requirement is usually interpreted to mean, "check the hash code of the installed software against the reference hash code held by the EAC or the State."

But ES&S's hash-checker doesn't do that at all. Instead, ES&S instructs its techs to create some "golden" hashes from the first installation, then subsequently check the hash code against these. So whatever software was first installed gets to be "golden", regardless of whether it's been approved by the EAC or by the State of Texas. This design decision was probably a convenient shortcut by engineers at ES&S, but it directly violates the EAC's rules for how hash-checking is supposed to work.

So, what have we learned?

We already knew that hash codes can't protect against hackers who install vote-stealing software, because the hackers can also install software that lies about the hash code. But now we've learned that hash codes are even more useless than we might have thought. This voting-machine manufacturer

- has a hash-code checker that erroneously reports a match, even when you forget to tell it what to match against;
- checks the hash against what was first installed, not against the authorized reference that they're supposed to;
- and the vendor insists on running this check itself — not letting the customer do it — otherwise the warranty is voided.

As a bonus we learned that the EAC certifies voting systems without checking if the validation software functions properly.

Are we surprised? You know: *fool me once, shame on you; fool me twice, shame on me.* Every time that we imagine that a voting-machine manufacturer might have sound cybersecurity practices, it turns out that they've taken shortcuts and they've made mistakes. In this, voting-machine manufacturers are no different from any other makers of software. There's lots of insecure software out there made by software engineers who cut corners and don't pay attention to security, and why should we think that voting machines are any different?

So if we want to trust our elections, we should vote on hand-marked paper ballots, counted by optical scanners, and recountable by hand. Those optical scanners are pretty accurate when they haven't been hacked — even the ES&S DS200 — and it's impractical to count all the ballots without them. But we should always check up on the machines by doing random audits of the paper ballots. And those audits should be "strong" enough — that is, use good statistical methods and check *enough* of the ballots — to catch the mistakes that the machines might

make, if the machines make mistakes (or are hacked). The technical term for those "strong enough" audits is ***Risk-Limiting Audit***.

Andrew W. Appel is Professor of Computer Science at Princeton University.

Susan Greenhalgh is Senior Advisor on Election Security at **Free Speech For People**.

FILED UNDER: UNCATEGORIZED

Comments

Douglas W. Jones says:
March 5, 2021 at 9:55 am

Regarding the local officials conducting acceptance testing: The fundamental problem with this is that most counties do not have the expertise to do this. Large urban counties with hundreds of precincts should have an election staff that includes people with real expertise. I've been in the election offices in Washington DC, Miami, Phoenix, Cleveland and places like that, and they really do have people on staff with the ability to do such testing. On the other hand, for each large urban county, there are tens of rural counties, many with just a handful of precincts. Those counties generally have no technical expertise in house and must outsource essentially everything technical, and they typically have no expertise to oversee their outsourcing contractor or contractors. They naturally gravitate to a vendor offering "one stop shopping." The acceptance testing issue demonstrates why this is a big mistake, but we need to find an alternative.

Back when I was chairing the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, I suggested that small counties should for consortia, sharing an election office between enough counties that they could afford staff with real expertise. They do this with things like maintenance depots for trucks and snow plows, why can't they do it for voting machines? My suggestions in this regard fell on deaf ears.

We have 8 states and several territories with populations below a million. The populations of Wyoming and Vermont are each smaller than the Des Moines metro area. It's impolite to wonder if those states have the necessary technical staff at the state level to do a competent job of acceptance testing. The District of Columbia is only slightly larger, but its election office combines both state-level and local election offices in one organization, and they do have significant technical staffing.

Having significant technical staffing does not imply that that staff is up to the job. I was consulting with the DC election office very shortly before Alex Halderman's students hacked the DC Internet Voting system during their public demo. At the same time I was observing the presence of significant technical expertise, he was demonstrating the kinds of things those experts were mismanaging, as he gained control of the Internet routers in the election office and the security cameras in the server room. My impression was that the DC election office was about as good as it gets, while Halderman and his students demonstrate that that really isn't good enough.

Michael says:
March 5, 2021 at 12:49 pm

What if the hashing function were itself implemented in hardware? Fundamentally there's no reason to implement a hashing algorithm in software, so you could make a dedicated piece of silicon that would calculate the hash fingerprint of the entire contents of the *rewritable store where the actual* voting firmware were held, which could itself by connected a fixed, tamper-evident bus; at that point an auditor could push a button, read the resulting hashed bytes straight off a dedicated register, and compare that to a hash of the voting firmware from the manufacturer. A separate dedicated module could do the same thing using a different hashing algorithm; keep adding discrete modules and hashing algorithms until sufficiently comfortable that whatever is on the firmware disk is either the manufacturer's software or someone has supply-side hacked multiple silicon foundries.

There are plenty of excellent reasons not to move to electronic voting, but I'm pretty sure we can establish that the current state of the bytes on some storage medium is identical to some other known and trusted state of bytes without relying on hackable software. Personally my bigger worry would be the auditors and authorities, all of whom are considerably more difficult to secure from corruption.

David Jefferson says:

March 5, 2021 at 3:01 pm

Excellent article. Thank you very much for publicizing this ludicrous situation.

The article says that Brian Mechler found a bug in the hash checking script, but I presume that does not cover the embedded hash algorithm it calls. Any such algorithm used for calculating the hash values in the National Software Reference Library should be a well-known *cryptographic* hash, but it does not sound like the EAC requires that. It is not clear to me what ES&S actually implemented. Also, the entire hash-checking process should be open source, even if all of the rest of the code is closed. It is hard to find any justification for keeping that short piece of code proprietary, and there is no way to trust the verification process if the hash algorithm code itself is secret.

In the end, as you say, it is crucial not to base our trust in elections on any kind of trusted software, but on strong and robust post-election risk-limiting audit process.

Susan Greenhalgh says:
March 5, 2021 at 4:13 pm

IIRC the VVSG requires that the algorithm be a specific NIST cryptographic hash. To your second point, the hash script and the hashing process are included in the vendor's Technical Data Package or TDP. And, unsurprisingly, the whole TDG is considered proprietary and is not public.

Susan Greenhalgh says:
March 9, 2021 at 9:04 am

An interesting addendum – the EAC's negligence here looks even worse when cast against a recommendation and warning that the GAO issued several years ago, specifically warning that the EAC should be defining test parameters and requiring testing of the software validation scripts. The GAO wrote:

"...the EAC has not established procedures and review criteria for evaluating the effectiveness and efficiency of manufacturer-provided voting system comparison tools. The Program Director told us in September 2012 that the commission requires voting system test laboratories to evaluate such tools and ensure they operate as intended by the manufacturer. However, the commission does not require that manufacturers or testing laboratories apply a standard set of evaluation criteria or test procedures to the tools and the commission has not developed any. Consequently, election jurisdictions still lack an independent framework for determining the accuracy, reliability, security, and usability of manufacturers' software verification tools. The absence of both of these elements of a robust software verification program means that state and local jurisdictions still lack the means to effectively and efficiently verify that voting systems used in federal elections are the same as those certified by EAC."

P.S. Thanks David!

Eric Valk says:
March 16, 2021 at 9:54 am

Hash checking can give a high level of security if implemented properly; EAC didn't even come close to a secure implementation. For example, Apple does a very good implementation on its handsets and computers. Micrsoft and IBM are also using this technology.
These things have to be part of such a solution
*Hash checking of the operating system code (SW) has to be done before the operating system is loaded. (This may have to be done in stages)
*Hash checking code, and other security keys must be stored in a "secure enclave", memory which cannot be modified or read except by a few SW commands not available to the operating system itself.
*The reports of the checking have to be in an encrypted message which includes sequence, date and time (created by code in the secure enclave) so that the receiver can determine if the message has been copied and replayed.

than says:
March 17, 2021 at 6:12 pm

While the technical aspects are interesting, the fact that the voting public does not possess the ability to independently verify the functioning of the voting system is itself problematic.

Jennifer Hofmann says:

March 19, 2021 at 12:30 pm

Thank you so much for this thorough report. We've turned it into an action asking the EAC to address these concerns and again advocate for hand-marked paper ballots. This will go out on Sunday to about 50,000 Americans (AmericansofConscience.com), but feel free to contact me if you have any questions. Thank you!

The State of Texas

Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.texas.gov

Ruth R. Hughs
Secretary of State

Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

REPORT OF REVIEW OF ELECTION SYSTEMS & SOFTWARE EVS 6.1.1.0 SYSTEM

PRELIMINARY STATEMENT

On August 21, 2020, Election Systems & Software ("ES&S" or the "Vendor") presented the EVS 6.1.1.0 system for examination and certification. The examination was conducted in Austin, Texas. Pursuant to Sections 122.035(a) and (b) of the Texas Election Code, the Secretary of State appointed the following examiners:

1. Mr. Tom Watson, an expert in electronic data communication systems;
2. Mr. Brian Mechler, an expert in electronic data communication systems;
3. Mr. Brandon Hurley, an expert in election law and procedure; and
4. Mr. Charles Pinney, an expert in election law and procedure.

Pursuant to Section 122.035(a), the Texas Attorney General appointed the following examiners:

1. Dr. Jim Sneeringer, an expert in electronic data communication systems; and
2. Ms. Lesley French, an employee of the Texas Attorney General.

At the time of the examination, the Office of the Secretary of State was closed to the public due to health and safety concerns relating to the novel coronavirus (COVID-19). As a result, certain procedures were implemented for the examination of the EVS 6.1.1.0 system. For example, the examination was held in a manner that allowed some of the examiners to participate in person and other examiners to attend remotely via live video conference. The examiners who were not physically present in the exam room were able to view the other examiners' interactions with the equipment and ask questions to the in-person examiners and the vendor. Mr. Pinney and Ms. French attended the examination in person, while the other examiners participated via live video conference.

The examiners witnessed the installation of the EVS 6.1.1.0 software and firmware that the Secretary of State's office received directly from the Independent Testing Authority. The Vendor then demonstrated the system and answered questions presented by the examiners. After the vendor presentation, the in-person examiners conducted a test election and tested various other components of the system with the participation and guidance of the examiners who attended remotely via live video conference.

Examiner reports regarding the EVS 6.1.1.0 system are attached hereto and incorporated herein by this reference.

On December 9, 2020, pursuant to Section 122.0371 of the Texas Election Code, the Office held a public hearing, by telephone, for interested persons to express views for or against the certification of the EVS 6.1.1.0 system.

BRIEF DESCRIPTION OF EVS 6.1.1.0

The EVS 6.1.1.0 system is an updated version of the EVS 6.1.0.0 system, which the Office certified in April 2020 for use in Texas elections. EVS 6.1.1.0 includes software enhancements to the existing election management system, but there were no updates to the firmware or hardware of the voting devices presented in the EVS 6.1.0.0 system.

EVS 6.1.1.0 has been evaluated at an accredited independent voting system laboratory for conformance to the 2005 Voluntary Voting System Guidelines (VVSG). EVS 6.1.1.0 was certified by the Election Assistance Commission (EAC) on July 27, 2020.

The components of EVS 6.1.1.0 are as follows:

Component	Version	Description
ExpressTouch	1.0.3.0	Direct-recording electronic voting machine (only for curbside voting)
DS200	2.30.0.0	Precinct scanner
DS450	3.4.0.0	Central scanner
DS850	3.4.0.0	Central scanner
ExpressVote (HW 1.0)	4.0.0.0	Ballot marking device
ExpressVote (HW 2.1)	4.0.0.0	Ballot marking device
ExpressVote XL	1.0.3.0	Ballot marking device
ElectionWare	6.0.1.0	Election management software
ExpressLink	2.0.0.0	Election management software
Event Log Service	2.0.0.0	Election management software
ExpressVote Activation Card Printer	N/A	Voting machine ballot activation device
ExpressVote Previewer	4.0.0.0	Election management software
PaperBallot	6.0.0.0	Election management software
Removable Media Service	2.0.0.0	Election management software
Toolbox	4.0.0.0	Election management software

FINDINGS

The following are the findings, based on written evidence submitted by the Vendor in support of its application for certification, oral evidence presented at the examination, and the written reports of the voting system examiners (all of whom recommended certifying the EVS 6.1.1.0 system for use in Texas elections).

The EVS 6.1.1.0 system, including its hardware and software components, meets the standards for certification as prescribed by Section 122.001 of the Texas Election Code. Specifically, the EVS 6.1.1.0 system and its components, among other things:

1. Preserve the secrecy of the ballot;
2. Are suitable for the purpose for which they are intended;
3. Operate safely, efficiently, and accurately and comply with the voting system standards adopted by the Election Assistance Commission;
4. Are safe from fraudulent or unauthorized manipulation;
5. Permit voting on all offices and measures to be voted on at the election;
6. Prevent counting votes on offices and measures on which the voter is not entitled to vote;
7. Prevent counting votes by the same voter for more than one candidate for the same office or, in elections in which a voter is entitled to vote for more than one candidate for the same office, prevent counting votes for more than the number of candidates for whom the voter is entitled to vote;
8. Prevent counting a vote on the same office or measure more than once;
9. Permit write-in voting; and
10. Are capable of providing records from which the operation of the voting system may be audited.

CONCLUSION

Accordingly, based upon the foregoing, I hereby certify Election Systems & Software's EVS 6.1.1.0 system for use in Texas elections.

Signed under my hand and seal of office, this 8th day of January 2021.

JOSE A. ESPARZA
DEPUTY SECRETARY OF STATE

U. S. ELECTION ASSISTANCE COMMISSION
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

January 28, 2021

Sent via e-mail

Steve Pearson, Senior Vice President of Certification
Election Systems & Software
11208 John Galt Blvd.
Omaha, NE 69137

Re: ExpressVote 1.0 Trusted Build

Dear Mr. Pearson,

On September 23, 2020, the U.S. Election Assistance Commission (EAC) was notified by the Texas Secretary of State's office that a voting system they were examining for certification, ES&S EVS 6.0.3.0, was displaying a hash validation error during trusted build installation on the ExpressVote 1.0. When questioned by Texas SOS representatives, the ES&S representative replied that this was expected behavior and that it also existed in EVS 6.0.2.0. Both versions are certified by the EAC to VVSG 1.0 and EVS 6.0.2.0 is currently deployed in 43 counties in Texas. 18 of the 43 counties use a configuration of EVS 6.0.2.0 that includes the ExpressVote 1.0.

Section 5.5 of the EAC's Testing and Certification Program Manual describes the trusted build as follows:

5.5. Trusted Build. A software build (also referred to as a compilation) is the process whereby source code is converted to machine-readable binary instructions (executable code) for the computer. A "trusted build" (or trusted compilation) is a build performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code. The primary function of a trusted build is to create a chain of evidence which allows stakeholders to have an approved model to use for verification of a voting system. Specifically, the build will:

5.5.1.Demonstrate that the software was built as described in the TDP.

5.5.2.Show that the tested and approved source code was actually used to build the executable code used on the system.

5.5.3.Demonstrate that no elements other than those included in the TDP were introduced in the software build. The vendor or source from which each COTS product was procured must be included in the TDP.

5.5.4.Document for future reference the configuration of the system certified.

5.5.5.Demonstrate that all COTS products are unmodified by requiring the VSTL to independently obtain all COTS products from an outside source.

As part of EAC certification, manufacturers are required to submit system identification tools and procedures that use hashes to prove that the applications installed on a voting system exactly match the certified versions.

The ES&S representative performing the installation during the examination used a method that was not tested by an EAC-accredited voting system test laboratory (VSTL) or certified by the EAC to install the software. When questioned by the Texas SOS representatives, the representative claimed that the installation method was reviewed/approved by the lab as part of their certification. Both SLI (VSTL for EVS 6.0.2.0) and Pro V&V (VSTL for EVS 6.0.3.0) deny that they had reviewed this installation method as part of certification testing.

Texas contracted with Pro V&V to verify ES&S' claim that the SYSLOAD.BMP file was the only change to the certified version. On September 24th, Pro V&V confirmed via source code review that this was the only change to the software. Texas has demanded that ES&S visit all 18 counties impacted by this deviation to perform a clean installation of the software using the certified installation procedure on all ExpressVote 1.0 machines (720 total).

We were under the initial impression that only EVS 6.0.2.0 systems in Texas were impacted. We now know that is not the case but need to fully understand all of the systems that are impacted.

In order to be in compliance with our Testing and Certification Program, we are requesting the following information. We may request additional information, and expect that you will disclose any other information that would assist us in understanding the scope of impact of any ES&S voting system regarding compliance with EAC certification.

1. The total number of jurisdictions throughout the United States affected including the jurisdiction name, contact information, and a list of affected devices including the system version information as well as serial numbers in each jurisdiction and when the installation occurred by ES&S personnel.
2. A detailed document providing a timeline of when this issue was first known and what ES&S is doing to remediate the issue.
3. All communication with the VSTLs regarding this issue.
4. An advisory notice specifying each EAC-certified voting system that uses the ExpressVote 1.0 and the ExpressVote's certified hashes and the mismatched hashes generated from the "update" file that has been installed on fielded devices.
5. A detailed document describing why ES&S disagrees with some of the statements the Texas Secretary of State's office made in the their letter to ES&S dated September 24, 2020.
6. ES&S' plan to install EAC-certified software on the affected ExpressVotes in Texas.
7. ES&S' plan to install EAC-certified software on affected ExpressVotes as requested by jurisdictions.
8. ES&S' planned resolution, including a documented procedure, to ensure that this does not occur again.
9. ES&S' communication plan and any other documentation (timeline, FAQs) that will be distributed to the affected jurisdictions for review and approval by the USEAC.
10. ES&S will communicate directly with the Executive Director or her designated representative and will cease to contact EAC employees throughout the duration of this investigation.

Finally, according to Section 5.15.4 of the Testing and Certification Program Manual, a manufacturer has 15 days from receipt of this letter to comply with the recommended corrective actions. However, due to the urgent nature of this issue and its impact on fielded, EAC-certified voting system 35 days before the 2020 General Election, we are requesting this information by close of business on October 1, 2020. Failure to comply will result in the EAC taking immediate required action as it deems appropriate as the system no longer complies with its original certification, including but not limited to initiating decertification actions and/or suspension of manufacturer registration.

We are taking this matter very seriously and understand that ES&S does as well and appreciate a prompt response given the nature of this issue.

Sincerely,

Mona Harrington, Executive Director

cc:
Kevin Rayburn, General Counsel
Jerome Lovato Director, Voting System Testing and Certification