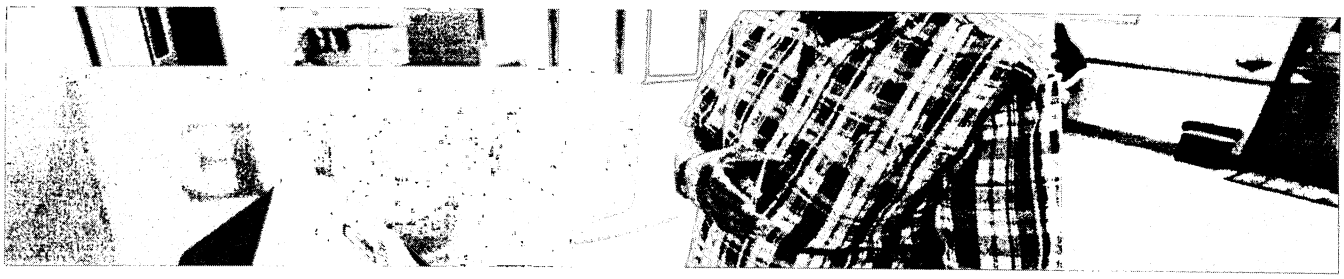


Walter Greene Jr. ponders his vote as Bastrop County election officials host an open house in Cedar Creek, TX, on September 1, 2020, giving a preview of new ExpressVote electronic voting machines slated for the crucial November elections. Photo credit: © Bob Daemmrich/ZUMA Wire

ELECTIONS

Election Assistance Commission Investigated ES&S Voting Systems

JENNIFER COHN 03/08/21

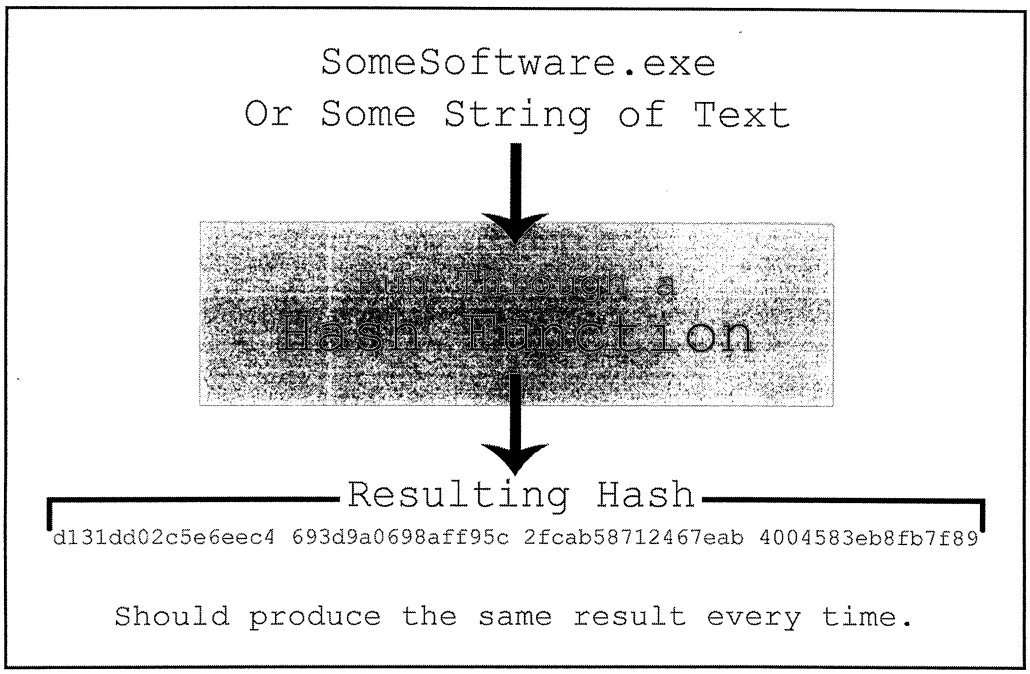
While allies of former President Donald Trump have leveled spurious charges against Dominion Voting Systems surrounding the 2020 elections, they have generally turned a blind eye to questions about Election Systems and Software, LLC (ES&S), a much larger voting machine company operating in *dozens of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

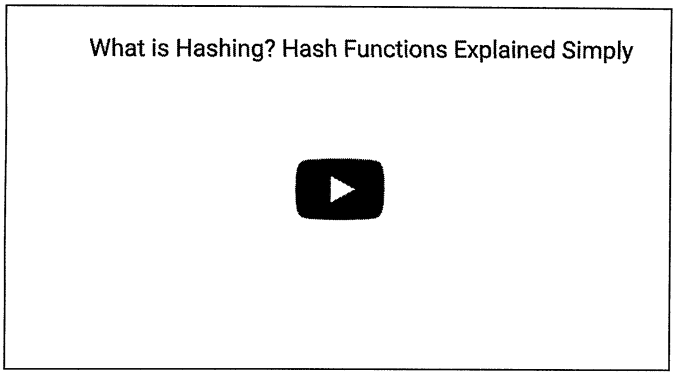
The shifting number of affected ES&S systems raises the question of whether some affected systems did not receive proper software installation and hash-validation testing before the 2020 election. At a minimum, it warrants explanation. But the EAC and ES&S have declined to comment for this story. Although *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

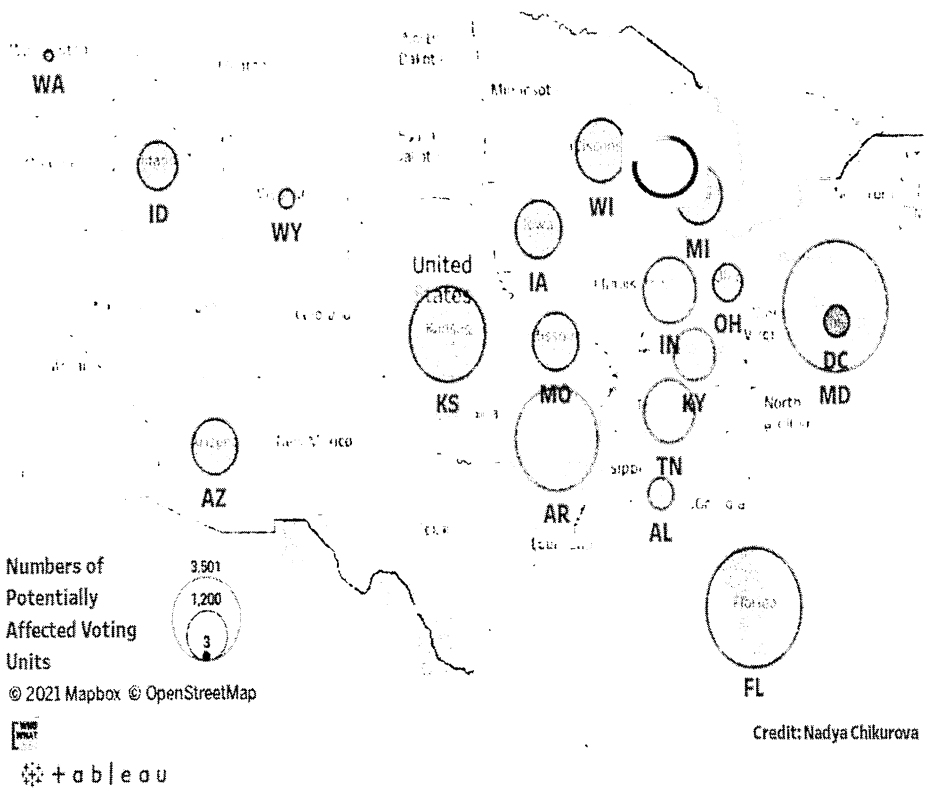
was not present. This was the expected result, and, as such, is considered a match. ... There has never been an issue to report and it is disheartening to think your team would doubt our integrity in this matter."

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."

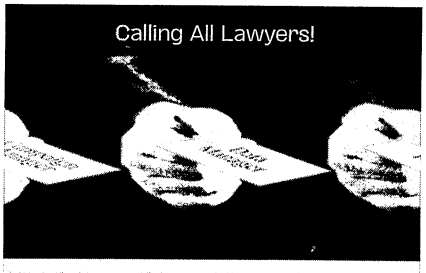
In 2019, House Democrats passed the Securing America's Federal Elections (SAFE) Act, which would have required robust manual audits called risk-limiting audits for all federal races and banned most of the current generation of touch screens, including the ExpressVote. But the GOP blocked the SAFE Act.

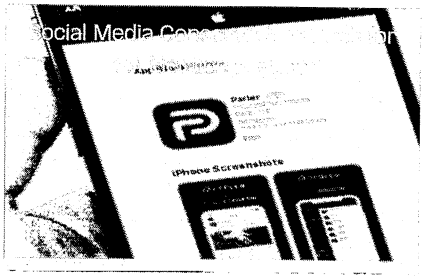
According to the National Voting Rights Task Force (in full disclosure, the writer is a member of said group), hand-marked paper ballots are preferable to touch screens for in-person voting, with an exception for voters with disabilities, because they are "quicker, safer, and inherently verified by the 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.

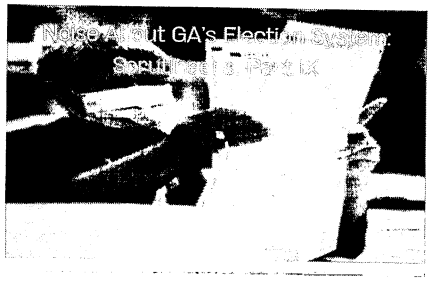
For more of WhoWhatWhy*'s work on Protecting Our Vote, see our Student Voter Guide and our series America Decides 2020. You can also find out the darker secrets behind our voting systems in our recently published e-book* Is This Any Way to Vote?: Vulnerable Voting Machines and the Mysterious Industry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