SUPERIOR COURT
OKANOGAN COUNTY

James M. Miller, Citizen Petitioner, vs. SECRETARY OF STATE, KIM WYMAN Respondent	Case No. **PROVIDE AN UNBROKEN HUMAN CHAIN OF CUSTODY TO VERIFY IDENTITY, COLLECT, TALLY, CERTIFY, REPORT AND IMMEDIATELY PUBLISH THE LOCAL TALLY CARDS FOR ALL ELECTION RESULTS AND NOT USE ELECTRONIC DEVICES OF ANY KIND**

WRIT OF MANDAMUS

/S/ James M. Miller

James M Miller, Citizen Petitioner
1 Blue Sky Place
Omak, WA 98841
(425) 471-8101
jmiller@leader.com

August 6, 2018

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Statutes & Rules

Other Sources

Ramsey Touchberry. (Jul. 17, 2018). Election Hacking: Voting-Machine Supplier Admits It Used Hackable Software Despite Past Denials. *Newsweek*.

Staff. (Jun. 12, 2008). SEQUOIA VOTING SYSTEMS, INC. USES VOTE-COUNTING SOFTWARE DEVELOPED, OWNED, AND LICENSED BY FOREIGN-OWNED SMARTMATIC, A COMPANY LINKED TO THE VENEZUELAN GOVERNMENT OF HUGO CHÁVEZ. National Institute of Standards (NIST).

Lord Mark Malloch-Brown. (Jun. 04, 2018). Biography & Timeline. *Americans for Innovation*.

Senator Ron Wyden. (Jul. 11, 2018). Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers. Ron Wyden.

Kim Wayman. (Accessed Aug. 06, 2018). System Security. Washington Secretary of State Website. (Microsoft totally controls the Washington State election information technology infrastructure).

Don Reisinger. (Oct. 17, 2017). This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings. Fortune.

Staff. (Accessed Aug. 06, 2018). Our Supporters. Center for American Progress.

INTRODUCTION

Chain of custody in the current election process does not satisfy the Rules of Evidence, is not bipartisan, and relegates citizens to mere spectators.

The Constitution of the State of Washington, Article I, Declaration of Rights, Section 19, Freedom of Elections states:

> "All Elections shall be free and equal, and no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage."

Petitioner received an initial response to his inquiries into election processes. Exhibit A.

Statistical sampling of the vote cannot satisfy the rules of evidence because it cannot count all the votes, which is the only standard that can apply. State v. Campbell, 691 P. 2d 929 - Wash: Supreme Court 1984.

Petitioner has concluded that the current Washington State election process has been developed through administrative overreach that contravenes the law that says use of voting machines (instead of bipartisan human vote counters) can only be made by legislative decision. The use of electronic voting machines has *never* been the subject of a robust public debate on the most sacred of our citizen‘s rights—the right to free and fair elections. Remarkably, no unbroken bipartisan chain of custody exists in the current election process. In addition to common sense, the law says this chain of custody must satisfy the Washington Rules of Evidence, among them are WAC 434-662-060, WAC 434-250-110, WAC 434-261-050.

Worse, with our mail-in ballot process, we have no way to even determine a voter‘s identity and qualification to vote, who actually marked the ballot? Are they a citizen, do they live in the state? Are they even alive? Were they bussed in? Have they voted multiple times? Is this actually a person‘s pet named "Steve" voting? *No one knows*. Therefore, the Rules of Evidence

cannot be satisfied in any regard. The current move to do statistical sampling cannot possibly stop the onslaught of fraud that our current system invites.

No actual human counting of the mail-in ballots occurs in the current voting processes under the control of the Washington Secretary of State. Administrative authority, instead of legislative authority, has been relied upon to implement voting machines. These machines are whole *replacements* for bi-partisan chains of custody. This administrative overreach without legislative inclusion, is clearly unconstitutional; the 'will of the people' has been put in jeopardy.

Instead, citizens are merely spectators. The actual counting, tallying and reporting processes themselves are done inside computer software that is completely under the control of county supervisors and staff—who are generally partisans of the party currently in power, and therefore, not bipartisan by nature.

1. **Unseen digital bits cannot survive the Rules of Evidence regarding chain of custody.**

The vote counting function resides solely as *unseen digital bits* inside a vote-counting computer with *no human verification* performed at the time of the vote. In the current election system, while one might vote for Candidate A, the unseen software can easily change that vote to Candidate B. No bipartisan group can check for such fraud.

Brenda Galarza, Records/Public Disclosure Officer on Jun. 29, 2018 confirmed that no bipartisan chain of custody exists. **Exhibit B**.

2. **United States election assistance commission *substituted* for bipartisan chain of custody by Washington State citizens.**

Ms. Galarza says that the State has replaced a bipartisan investigation of electronic voting devices and software in our state with a *federal* break in the bipartisan chain of custody by ~~–an~~ independent testing authority designated by the United States election assistance commission" citing RCW 29A.12.080.

This statute violates the sovereignty of Washington State citizens‘ over our elections—and thus breaks the chain of custody. *See* RCW 29A.12.030 (“The secretary of state [not the federal government] shall inspect, evaluate, and publicly test all voting systems or components of voting systems”). The federal government has no authority to be involved in this important State‘s rights issue. This is a flagrant abuse of State‘s Rights on the Washington State vote.

3. "Two county auditor staff"*substitute* for bipartisan chain of custody.

Ms. Galarza says "inappropriate or unauthorized access to the secured ballot materials and must be accompanied by at least two county auditor staff at all times. (WAC 434-261-045, WAC 434-250-110 & RCW 29A.40.110)."

This statement affirms that no bipartisan chain of custody is used. “Two county auditor staff” is not a bipartisan chain of custody.

Also, no procedure exists for bipartisan verification that the person or entity that mailed in the ballot is who he or she purports to be, or that he or she is qualified to vote.

4. No citizen sees a "verifiable paper ballot" after the electronic scan.

Ms. Galarza says that each voting device "must produce a voter verifiable paper ballot." This procedure is not followed and can only be considered willfully misleading. While she quotes the statute, this is not what happens.

All Washington citizens receive paper ballots in the mail. They do not use electronic voting machines to place their vote. See RCW 29A.40.020. Therefore, no citizen receives, or can verify, the electronic scan that occurs *after* the ballot is received back in the mail. In our state this opportunity for fraud is worse since, with mail-in ballots, we don‘t even know if the person who mailed it is real or qualified to vote. The counting is totally in the dark. This process is another break in a bipartisan chain of custody. In short, there is *no bipartisan chain of custody comparison* of the ballots whatsoever.

Article 1, Section 1 of the Washington Constitution states:

> "**All political power is inherent in the people**, and governments derive their just powers from the consent of the governed and are established to protect and maintain individual rights." (Emphasis added).

Washington citizens are being forced to rely on *pure speculation* that the electronic machinery used to verify the voter's identity, as well as scan, count and report the ballots are accurate. Bipartisan citizen counters are not part of the process.

5. <u>The current voting process *forces* election administrators to commit fraud since they cannot certify any vote in any county. In short, speculation of the integrity of a vote counting machine does not satisfy the Rules of Evidence regarding chain of custody</u>.

In the current election procedures, our state election judges are required to accept the unilateral word of private voting machine vendors who have allegedly validated a federal commission. Such outside certifications of our election devices, by nature, fail to ensure an unbroken bipartisan chain of custody required by the Washington State Constitution.

Vendor and federal statements of certification utilized by our officials should be more accurately defined as statements of faith, since they are relied upon in place of bipartisan review by citizens.

The claims made by election officials to Petitioner are largely false and thus at odds with the statutes. For example, the Washington Supreme Court stated in *Armendariz*:

> ¶ 8 Where the plain language of the statute is subject to more than one reasonable interpretation, it is ambiguous. *Cockle v. Dep't of Labor & Indus.*, 142 Wash.2d 801, 808, 16 P.3d 583 (2001). This court may attempt to discern the legislative intent underlying an ambiguous statute from its legislative history. Id. Likewise, this court may look to authoritative agency interpretations of disputed statutory language. *Port of Seattle v. Pollution Control Hearings Bd.*, 151 Wash.2d 568, 593, 90 P.3d 659 (2004). *State v. Armendariz, 156 P. 3d 201* (Wash. SC 2007).

Therefore, since the responses I received are ambiguous at best, this Court has the authority and duty to grant this writ to prevent prejudice against the citizens for a fair vote.

6. **Senator Patty Murray agrees that we must discard electronic voting, use paper ballots and insure unbroken, bipartisan chain of custody.**

Senator Patty Murray (D-WA) recently introduced "The Protecting American Votes and Elections Act" *mandating paper ballots* and *risk-limiting Audits*. She stated just weeks ago on Jun. 12, 2018:

> "With known vulnerabilities and a clear history of foreign interference, it is critical we take meaningful steps to protect the integrity of our elections and ensure the public's faith in our voting system." **Exhibit C**.

Why wait? A reasonable person will ask why Senator Murray did not first move to fix *Washington's* election system long ago? Nevertheless, this writ will remedy her delay in addressing *our* sovereign need to protect *our* elections.

According to Stuart Holmes, Voting Information System Manager, Office of the Secretary of State, fifteen percent (15%) of our electronic voting machines are provided by ES&S. Exh. C.

7. **Washington vote counting vendor ES&S *admits* a secret backdoor that can be exploited by hackers.**

ES&S just admitted to Senator Ron Wyden (D-OR)—after multiple prior denials—that they have secretly embedded the software program PCAnywhere in their voting machines, ostensibly to allow their engineers to maintain their devices remotely. This excuse rings hollow since ES&S lied about the presence of this backdoor access. The reality is that *any* programmer of normal skill in the art—not just ES&S programmers—can access these networked or standalone machines through preinstalled firmware and media voting devices if they have the

correct username and password. See *Newsweek*, July 17, 2018 [1] This fact alone shows sufficient *prima facie* risk to grant this writ. **Exhibit J**.

Further, on July 11, 2018, Senator Wyden testified to the U.S. Senate Rules Committee and published a Senate statement subtitled: Testifying at Senate Rules Committee, Wyden Blasts Voting Machine Manufacturers, Calls for Passage of His Bill Mandating Paper Ballots. [2]

8. Dubious OpTech software is contained in many Washington State voting machines.

On Jul. 23, 2018, Petitioner was told by Stuart Holmes, Voting Information Systems Manager, Office of the Secretary of State that "Smartmatic voting systems are not certified or used in the State of Washington." Exh. B.

However, the software engine inside Smartmatic is OpTech. OpTech software is also used in similar systems that *are* used in Washington, including ES&S (6 out of 39), Sequoia and Hart InterCivic (20 out of 39). **Exhibit E**

See also Angela Gunn. (Nov. 1, 2006). E-voting and voter registration: The vendors - Who's building the gear that's running the show? *Computerworld*. **Exhibit F** (–Smartmatic Corp., is privately owned, with a controlling interest held by founder and CEO Antonio Mugica. Mugica holds dual Spanish and Venezuelan citizenship. Sequoia offers AVC Edge and AVC Advantage DRE units, an AVC Edge DRE/VVPAT unit, and sells a Sequoia-branded Optech Insight optical scanner" and "Election Systems & Software also offers an Optech line").

---

[1] Ramsey Touchberry. (Jul. 17, 2018). Election Hacking: Voting-Machine Supplier Admits It Used Hackable Software Despite Past Denials. *Newsweek*. https://www.newsweek.com/election-hacking-voting-machines-software-1028948

[2] Senator Ron Wyden. (Jul. 11, 2018). Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers. Ron Wyden. https://youtu.be/XQzsoJSAtA4 ; *See* also https://www.wyden.senate.gov/news/press-releases/wyden-paper-ballots-and-audits-are-essential-to-secure-american-elections-against-foreign-hackers

9. **Proof of foreign interference in Washington State elections.**

Hart InterCivic used in the State of Washington licenses Sequoia's / Smartmatic's Optech Insight software originally developed in Venezuela.

See the National Institute of Standards (NIST) analysis which shows the real risk of foreign influence in our vote.[3]

Hart InterCivic licensee, Smartmatic is foreign-owned by SGO Corporation Limited (UK) / Smartmatic that is owned by British Privy Counselor associated with Lord Mark Malloch-Brown. Malloch-Brown is a close colleague of globalist George Soros who openly works to destabilize American elections. Malloch-Brown was a founding chairman of Soros' Open Society Foundation, vice President of Soros' Quantum Fund, and Vice Chairman of Soros' 'Soros Fund Management'. While Malloch-Brown was Deputy Secretary of the United Nations, he rented a Soros estate in upstate New York.

The involvement of Malloch-Brown and Soros in the OpTech licensing (inside ES&S and Hart InterCivic) shows an obvious threat of foreign interference in Washington State's elections. *See* Lord Mark Malloch-Brown Biography and Timeline. **Exhibit G**.

In Petitioner's FOIA questions, the state sidestepped the issue of the common OpTech software. This discrepancy begs the question as to how OpTech can be certified in ES&S and Hart InterCivic and not certified in Smartmatic. This ambiguity is deeply troubling, especially considering that ES&S's blatantly lied to Senator Wyden about their PCAnywhere backdoors. **Exhibit. I**.

---

[3] Staff. (Jun. 12, 2008). SEQUOIA VOTING SYSTEMS, INC. USES VOTE-COUNTING SOFTWARE DEVELOPED, OWNED, AND LICENSED BY FOREIGN-OWNED SMARTMATIC, A COMPANY LINKED TO THE VENEZUELAN GOVERNMENT OF HUGO CHÁVEZ. National Institute of Standards (NIST).
https://www.nist.gov/sites/default/files/documents/itl/vote/SequoiaSmartmaticReport61208.pdf

10. **Incurable Uncertainty – Numerous breaks in the bipartisan chain of custody must be cured before electronic voting can be relied upon, if ever.**

The State's current election procedures create an incurable uncertainty as to the veracity of the vote count since the process has numerous breaks in the bipartisan chain of custody as discussed herein, as highlighted by Senator Ron Wyden. *Supra*.

"Trust me" affirmations by election officials alone are inadequate to trust the vote tallies. **Counting the vote is the exclusive purview of the citizens themselves.** State bureaucrats have an *inbuilt conflict of interest* to have their bosses remain in power. Washington State's election machine processes suffer from an incurable uncertainty regarding the ballot vote tally process and results. In addition, as soon as a ballot is read into the scanner, the votes are *hidden*, secret and unable to be certified. **This is a break in the bi-partisan chain of custody**.

Put more simply, on election day, no identity validation is done, and no bipartisan *human* tally of the votes is used to audit the ballot scanning machines of the mailed in ballots.

All testing of electronic voting machines is done *a priori* (before a vote). No *post priori* (after the vote) testing is done. This too is a flaw in the certification and auditing processes. Common sense says that the current system is ripe for fraud.

11. **No honest engineer could certify electronic voting machines.**

Even as advancing technology and contemporary lifestyles drive evolution in our method of voting, Washington's statutory regime manifests clear legislative intent to assure that secrecy in the method of voting in every election is absolute.

The secret ballot must not devolve into a mere _state secret' held by officials promising not to tell. And yet, with the current technology, a state secret has occurred with the implementation of machine voting. No matter how many tests are done, the voter is dependent on speculation rather than bi-partisan, empirically observable phenomenon.

12. <u>The citizen sees nothing; the "observers" are mere spectators</u>.

The citizen cannot see the circuits, firmware, malware, or any software. The citizen sees NOTHING about how his or her vote is tallied. They are not present when the machines print a receipt, so they cannot check the scan for accuracy. The voter does not know if the software could detect when it was being tested and fool the testers—like the Volkswagen diesel fraud that hid poor emissions results from regulators for years. The software for the Volkswagen modified itself under test. **<u>Exhibit H</u>**. This very same possibility exists with all the election machines used by the State.

13. <u>Washington State voter's rights to a fair election should not be subjected to speculation as to the authenticity.</u>

Since no empirical human, bipartisan observation at all is part of this counting and reporting process, it is incurably uncertain.

The citizens of the State of Washington have no adequate remedy for this incurable uncertainty other than this Writ of Mandamus. The Secretary of State, Kim Wyman, must be compelled to:

(1) Verify the true identity and qualification of each voter to vote,

(2) Add human bipartisan counting of paper ballots where a voter submits the vote card and immediately has his or her finger dipped in suitable purple voting dye used around the world to ensure "one person, one vote,"

(3) Preparation of a tally sheet that is certified by the human bipartisan counters and immediately photographed and published on each county website,

(4) Hand delivery of that tally sheet to the state election tabulator by each group of county bipartisan election judges,

(5) Verification that the state election tabulator has entered the county's certified tabulation. This process must be done in lieu of or in addition to the use of electronic devices that can be used as an audit verification adjunct—but never again as the primary vote counting and tally processes.

The state will prevail without this injunction, as no remedy is being offered, and the will of the people is subject to the very real danger of interference in free and fair elections.

The benefit of this injunction outweighs any process utilized by the state, if that process thwarts the true and constitutional expression of the will of the people at the polling place.

The people of the State of Washington have the right of relief from this current state election process that evidently thwarts their constitutional rights.

It is the duty of the Secretary of State to provide a free election according to the Washington State Constitution without regard to any hardship such a duty imposes.

According to the Secretary of State, she recognizes the vulnerabilities in the State's elections processes that this writ addresses. This is more prima facie evidence of a problem whose solution appears to be being delayed for purely partisan political reasons.

Brenda Galarza, representing Kim Wyman, announced that voting irregularities will be addressed in 2019 using human statistical sampling of ballots. Exh. B.

First, why wait until 2019?

14. <u>Statistical sampling is easily fudged and does not replace unbroken bipartisan chain of custody sufficient to satisfy the Rules of Evidence.</u>

Second, why statistical sampling when we can just count and certify all votes in real time? Statistical sampling appears to be another euphemism for an excuse to hide rigged voting. Bipartisan human counting solves this problem.

State officials always use alleged cost savings to justify continued use of electronic machines. This argument is fallacious for several reasons.

First, the primary objective is a free and fair vote, not cost savings. **A fair vote—no matter what it costs—is the true objective.**

Second, bipartisan citizen volunteers needed to count the votes do not require payment for their services.

Third, it is very easy for bureaucrats to hide partisanship inside the cost savings argument.

Fourth, if vote counting takes a week or more, so be it. The rush to have election-night results only serves to hide and promote fraud and a rush to bogus judgment.

By the Senator Murray‘s and Secretary of State Wyman‘s admissions, the machine counts do not provide the certainty necessary to meet statutory requirements. Only a whole and complete, bi-partisan chain of custody human tally count of the ballots can overcome the incurable uncertainty of the existing processes.

Any process that is hidden and secret (like the ones currently used) is unconstitutional. In fact, the current processes force election judges in each county to certify a fraud, since they have not themselves counted the votes.

Statistical mathematics, silicon circuits, certificates of authenticity, incomplete responses to public records, protestations, and technical obfuscations are not logical or acceptable substitutes for direct human empirical observations operating under the constitutional principle of bi-partisan chain of custody.

The Petitioner also makes the claim that the decision to utilize electronic voting machines in any manner, has not been properly adopted by the state pursuant to *Ballasiotes v. Gardner, Supreme Court of Washington, March 18, 1982, No. 48295-1.* This court specifically addressed

the issue at hand. The current system is administrative by nature, and directly contradicts this opinion. The use of machines, by any county, electronic or otherwise, to replace the un-broken bi-partisan chain of custody is not supported, since electronic machines were never specifically debated and decided by the legislature.

The ignoring of *Ballasiotes* is *prima facie* evidence that no machines including electronic devices in the electoral process in counting the ballots are legal as they have not been properly adopted by the people. To be clear, the Petitioner is not contending that machines can't be used to transport ballots, move them around, or to publish pictures of tally sheets on the "Internet of Things"; the Petitioner is saying that machines can't be used in the bi-partisan counting and tally of the votes; the machines have not been 'properly adopted', and represent a premia facie break in the bi-partisan chain of custody; which is illegal in the State of Washington.

15. <u>Vote counting process is not bipartisan.</u>

Nowhere in WAC 434-260 ELECTION REVIEW PROCESS AND CERTIFICATION OF ELECTION ADMINISTRATORS is the vote counting process in the State of Washington bipartisan—meaning selected election administrators from each political party oversee the vote counting process. Rather, paid partisan employees of the Secretary of State do. This is yet more *prima facie* evidence that vote counting in the State of Washington is run by bureaucrats that can press their own agendas outside the electoral process. The opportunity for manipulation and fraud is evident.

It all depends on what the definition of "may" is

Instead, "observers" from parties merely watch the process like spectators at a baseball game with their beer and brats. See WAC 434-261-020. The break in the bipartisan chain of custody is quite evident in WAC 434-250-110. PROCESSING BALLOTS:

> "(6) Final processing of voted ballots, w*hich* ***may*** *include scanning ballots on an optical scan voting system*, may begin after 7:00 a.m. on the day of the election." (Emphases added).

This law implies that ballots are counted by humans. However, very evidently, the Secretary of State has relied upon the single word "may" for her overreaching authority that now counts ALL ballots electronically. A reasonable person will consider the substitution of ALL for MAY a willful misinterpretation of the statute, if not administrative abuse.

Since Petitioner has established that unseen, *unobservable* electronic bits and bytes in all electronic voting systems breaks the bipartisan chain of custody, the Washington State Statute itself proves that a break occurs at vote counting. This is more *prima facie* evidence why this writ must be granted.

Statistical sampling *implies* vote counting errors which CITIZENS DO NOT WANT!

The need for this writ is further reinforced by the most recent order by the Secretary of State to do statistical sampling of one race in three precincts in each county.[4] This process is mathematically meaningless. In mathematics, a statistical standard of deviation ***implies and***

[4] Kim Wyman. (Jul 16, 2018). Protecting Our Votes Means Strengthening Cybersecurity. The Aspen Institute. https://www.aspeninstitute.org/blog-posts/protecting-our-votes-means-strengthening-cybersecurity/; *See* also Kim Wyman. (Mar. 29, 2018). Washington to receive nearly #$8 million to upgrade elections systems. Washington Secretary of State. https://www.sos.wa.gov/office/news-releases.aspx#/news/1280

assumes errors in the vote counting! Predicative mathematical values in a statistical sampling are meaningless to a fair and accurate vote. **It assumes that it is not accurate!**

The 2004 HBO expose *Hacking Democracy* clearly shows how electronic voting machines can be tampered with *after* passing quality assurance testing.[5]

STATEMENT OF THE CASE

The previous discussion and law is fully incorporated herein. Counting votes in a bipartisan way is a founding principle of a Constitutional Republic. Unbroken chain of custody must satisfy the Washington State Rules of Evidence.

The Washington State Constitution states that that free elections without interference are a citizen‘s right. Any uncertainty in the count is unacceptable.

The burden to maintain the reliability of the vote is the highest and most solemn duty of a citizen in our Republic. It is the county auditor‘s duty to ensure that processes, as defined by the Secretary of State are properly enabled. Among these duties is the maintenance of a bipartisan chain of custody of the ballots and the counting of those ballots.

This maintenance should be by *empirical observation by humans*, who cooperate under lawful penalty to ensure that the ballots, as marked, are not compromised. Elections chain of custody refers to physical and electronic evidence controls for:

1. who can vote
2. who did vote
3. actual ballots as marked by each voter, and
4. evidence transfer and storage

The current process is highly prone to recounts and litigation because it departs dramatically from the statutory requirements.

---

[5] Hacking Democracy (2006). The Hack Trailer. *HBO*. https://youtu.be/t75xvZ3osFg

Proper accounting requires chain of custody measures, which auditors use to assess information reliability. Chain of custody is dictated by the Rules of Evidence. The current election processes do not comply at any point.

The current State of Washington process to maintain bi-partisan chain of custody fails under the current process. The reasons for the failure is very simple. First, the person‘s identity and qualification to vote cannot be verified. Then, the use of the electronic scanning machines causes the loss of bi-partisan chain of custody as soon as a ballot is scanned. While a paper receipt is created at the time of the scan, the voter is not present since the ballot was mailed in. So, the requirement for a printed receipt is nonsensical. The voter is treated more respectfully at Dairy Queen. At least they get a real receipt at DQ!

Further, in the current process no one knows if the person‘s name on the mail-in ballot is really that person. The notion that proper voters identification is somehow a burden on the citizenry is nonsensical. We show our identification every time we use a credit card, or cash a check, or sign up for Medicare or Medicaid.

In the current State of Washington voting process, no qualified voter is able to confirm that the scan of their ballot is accurate or is totaled accurately. The current system defies logic and commons sense.

There is no summation tally audit for the voting machines that scan the mailed in ballots. Further, the citizen‘s vote is not counted by bi-partisan humans.

This process is the definition of incurable uncertainty. No certificate of assurance from any entity, test, encryption, or machine language can prevent this loss of observation.

A human citizen voter cannot observe an integrated circuit, silicon chip, or the software programming embedded on the chip. Therefore, no one attests to an unbroken chain of custody.

A statistical sampling of the voting summation cannot cure this uncertainty since such samplings are based on totals that have not been prepared by bipartisan counters. On Aug. 06, 2018, Petitioner spoke with Jessica at the Okanogan County Auditor Office. She confirmed that a new statistical sampling of ballots will start occurring with the 2018 primary election on Aug. 07, 2018. However, she was unable to provide Petitioner with the bulletin from the Secretary of State that directed them to perform the new sampling.

The logic is simple . . . what the human eye cannot see, without concurrence under bi-partisan chain of control, is a fraud disguised by technology.

Evolving voting methods have produced systems that contain significant holes in chain of custody which call election legitimacy into question.

Three voting methods breach bipartisan chain of custody:

(1) vote-by-mail,

(2) electronic voting, and

(3) Internet voting.

These methods make it IMPOSSIBLE for the public to verify that:

(a) the voter is who they say they are and are qualified to vote,

(b) all ballots cast were counted;

(b) ballots counted were not altered; and

(c) unauthorized votes were not added.

Therefore, it is the duty of the Secretary of State, Kim Wyman, to provide a cure for this outrageous indiscretion regarding the expression of the will of the people. She should be compelled by this Court to direct each county: (1) to only allow counting of the mail-in ballots by bipartisan citizens groups who verify the valid identity of each voter, and (2) to post the tally

results on each county website so that the certified tally card is immediately observable by all citizens; the intent is to ensure "human ballot counting and tally" while maintaining observable bi-partisan chain of custody over the ballots themselves.

Remarkably, none of these public officials who responded to the Petitioner could provide evidence that the election machines themselves were safe from internal/external tampering, or that the processes surrounding the use of these machines were able to provide an unbroken, bipartisan change of custody.

It is evident that this assurance could not be provided because it cannot be verified. The petitioner‘s request for more information about the voting machines was denied under RCW 42.56.270, the Public Records Act.

Petitioner filed for administrative relief in court but was informed that he would be liable for all legal costs incurred by the vendor to respond, per the Okanogan County Prosecuting office.

Petitioner was provided the copious documentation about election processes and controls used by the State. **Exhibit K.** The necessity for this writ was made patently obvious after discovering the flaws in our processes that are large enough to drive a truck through.

16. Petitioner is a recognized expert in organization systems, procedures and processes

The Petitioner is a retired Boeing project manager who has been responsible for complex airplane critical and flight safety avionics software and hardware involving multiple-billion dollar projects. This makes him an expert in system processes, procedures and quality. The Petitioner hereby certifies that in his professional judgment, after studying all the information provided in this writ, the programs and processes used in the State of Washington voting processes are woefully inadequate and appear to be willfully so. Petitioner asserts that no honest process engineer could possibly certify what can best be described as a magical process that

could have only ever been intended to rig elections. Petitioner's firm conclusion is that the systems and procedures are so convoluted as to lead a process engineering expert to conclude that *mischief* is the only possible use and outcome of the current election system in the State of Washington. *See* Petitioner's expanded resume and expertise in **Exhibit L**.

17. Microsoft controls our data; Microsoft is not bipartisan

The Secretary of State's website under "System Security" states:[6] **Exhibit M**

> "Patch Management:
>
> The Quality Assurance (QA) system is patched the day after any "patches", "hotfixes", or "cumulative" updates are received from **Microsoft**. Production (prod) servers are patched after the system updates are fully tested in QA and authorized for deployment. In most cases, the production system patched two weeks after QA to allow for testing and verification.
>
> Elections Results Site
>
> The elections results are hosted in **Microsoft's** Azure cloud, which provides server and geographic redundancy." (Emphasis added.)

It is notoriously public knowledge that Microsoft is a partisan of far left-leaning organizations. *Fortune* magazine assessed Microsoft's political leanings stating:

> "Microsoft is another supporter of the Brady Campaign, which earned it low marks on 2nd Amendment rights. The tech giant was also hit for being 'a partner of The Nature Conservancy, a liberal and active proponent of cap-and-trade and a carbon tax.'
>
> In its evaluation of Microsoft, 2ndVote also says that the company supports organizations, like Center for American Progress and the League of United Latin American Citizens, which support sanctuary cities."[7]

---

[6] Exh. M. Kim Wayman. (Accessed Aug. 06, 2018). System Security. Washington Secretary of State Website. https://www.sos.wa.gov/elections/system-security.aspx

[7] Exh. N. Don Reisinger. (Oct. 17, 2017). This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings. *Fortune*; See also Staff. (Accessed Aug. 06, 2018). Our Supporters. Center for American Progress.

The Center for American Progress is notoriously known to have been founded by Democrat operative John Podesta, who is notoriously known to have intimate political ties to George Soros, Hillary Clinton, The Clinton Foundation and other far left-leaning political organizations.

A reasonable person can easily see that the Washington State election process is completely compromised by Microsoft‘s partisan control of vital elements of our election system. **Exhibit N**.

LAW & ARGUMENT

The previous discussion and law is fully incorporated herein. The current ballot scanning process in the State of Washington cannot guarantee that the tally is correct because it is not performed by humans. Voters do not even observe the electronic scanning in the counties. Humans only enter the ballot into the machine, and no human tally occurs outside of the machine, thus breaking the bi-partisan chain of custody empirical observation.

Petitioner, and the rest of the citizenry, have a right to rely upon the truthfulness of the statements of public officials. When those statements contradict the statutes, this Court can intervene. The Washington Supreme Court stated:

> ¶ 8 Where the plain language of the statute is subject to more than one reasonable interpretation, it is ambiguous. *Cockle v. Dep't of Labor & Indus.*, 142 Wash.2d 801, 808, 16 P.3d 583 (2001). This court may attempt to discern the legislative intent underlying an ambiguous statute from its legislative history. *Id.* Likewise, this court may look to authoritative agency interpretations of disputed statutory language. *Port of Seattle v. Pollution Control Hearings Bd.*, 151 Wash.2d 568, 593, 90 P.3d 659 (2004). *State v. Armendariz*, 156 P. 3d 201 - Wash: Supreme Court 2007 at ¶ 8.

This Court may grant relief when a state agency is acting erroneously and in contradiction to the statute. The Washington Supreme Court stated in *Port of Seattle*:

> This court may grant relief if we find that the PCHB [Pollution Control Hearings Board] order is "outside the statutory authority or jurisdiction of the [PCHB]" or

> if the PCHB has "erroneously interpreted or applied the law." RCW 34.05.570(3)(b), (d). Where statutory construction is necessary, this court will interpret statutes de novo. Pub. Util. Dist. No. 1, 146 Wash.2d at 790, 51 P.3d 744. *Port of Seattle v. PCHB*, 90 P. 3d 659 - Wash: Supreme Court 2004 at 669.

While equitable estoppel is not favored, as is request here, it is needed when a manifest injustice is threatened or is occurring, as is the case here. The Washington Supreme Court affirmed this in *Ecology*:

> Equitable estoppel against the government is not favored. *Id*. Accordingly, when the doctrine is asserted against the government, it must be necessary to prevent a manifest injustice and applying estoppel must not impair the exercise of government functions. *Id*. Proof of the elements of estoppel must be by clear, cogent and convincing evidence. *Id*. *State, Dept. of Ecology v. Campbell & Gwinn*, 43 P. 3d 4 - Wash: Supreme Court 2002 at 14.

The *Ecology* opinion describes a procedure for determining if a manifest injustice is occurring:

> Equitable estoppel may apply where there has been an admission, statement or act which has been justifiably relied upon to the detriment of another party. *Lybbert v. Grant County*, 141 Wash.2d 29, 35, 1 P.3d 1124 (2000); *Beggs v. City of Pasco*, 93 Wash.2d 682, 689, 611 P.2d 1252 (1980). Establishment of equitable estoppel requires proof of (1) an admission, act or statement inconsistent with a later claim; (2) another party's reasonable reliance on the admission, act or statement; and (3) injury to the other party which would result if the first party is allowed to contradict or repudiate the earlier admission, act or statement. *Theodoratus*, 135 Wash.2d at 599, 957 P.2d 1241. *Id*.

This writ satisfies the need for this Court to equitably estop the Secretary of State from engaging in fraudulent voting practices.

(1) "*an admission, act or statement inconsistent with a later claim*" - As shown above, the admissions and statements by public election officials are inconsistent with the statute and with the election system procedures and processes.

(2) "*another party's reasonable reliance on the admission, act or statement"* - Both Petitioner and all Washington citizens have reasonably relied upon the Secretary of

State‘s election procedures and processes as the sole supplier of these public services. Therefore, the Petitioner has no choice but to rely upon these statements as truthful and in compliance with the statutes.

(3) "*injury to the other party which would result if the first party is allowed to contradict or repudiate the earlier admission, act or statement*" – A reasonable person knows that elections have direct material consequences to the administration of our Constitution. Winning candidates are given real power and authority in our State as a result of these elections. The new evidence shows that these publicly-elected officials have been empowered on the basis of flawed, if not fraudulent, voting processes that *pretend* to be compliant with the statute. As a result, any mere repudiation of prior statements and admissions only further damages the Petitioner by allowing the officials to further obfuscate the true nature of our flawed elections systems. The damages to Petitioner and our State are only exacerbated and real bipartisan fixes are only delayed.

The responses received by state public officials refused to provide substantive information about the mechanics of the voting systems currently used. **Exhibit I**. The documentation provided by the Okanogan County Auditor‘s office is too voluminous to incorporate herein. Therefore, it will be made available upon request pursuant to Wash. R. Evid. 1006.

Purity of the Ballot

The Supreme Courtin Hanson affirmed the priority for purity that should motivate this Court to grant this writ:

> Our democratic system of free and fair elections hinges on enforcement of the Constitution‘s and Legislature‘s carefully constructed array of provisions securing

> for an absolutely secret method of voting. The Constitutional requirement of an absolutely secret ballot, independently and as implemented by statute, is fundamental. "The terms of the statute are absolute, explicit and peremptory; no discretion is given. They are designed to secure the secrecy and purity of the ballot, are mandatory in their character and binding upon the electors." *State ex rel. Hanson v. Wilson*, 113 Wash. 49, 52 (1920).

Voting: A Fundamental and Cherished Liberty

> "Voting is one of the most fundamental and cherished liberties in our democratic system of government." *Burson*, 504 U.S. at 213 (Kennedy, J., concurring).

Secretary of State may not compromise the vote

This writ calls for institution of an unbroken bipartisan chain of custody immediately.

Chain of Custody in Washington State law is defined as:

> "Chain of custody" means the documentation of the succession of offices or persons who held public records, in a manner that could meet the evidentiary standards of a court of law until their proper disposition according to an approved records retention schedule.
>
> The agency must maintain chain of custody of the record, including employing sufficient security procedures to prevent additions, modifications, or deletion of a record by unauthorized parties. If there is a break in chain of custody, it must be noted in the transmittal to the archives. WAC 434-662-060. Authentication and chain of custody of electronic records.

The Washington Supreme Court in *Campbell* states regarding chain of custody and the Rules of Evidence:

> [8] Before a physical object connected with the commission of a crime may properly be admitted into evidence, it must be satisfactorily identified and shown to be in substantially the same condition as when the crime was committed. *Brown v. General Motors Corp*., 67 Wn.2d 278, 285, 407 P.2d 461 (1965); *Gallego v. United States,* 276 F.2d 914, 917 (9th Cir.1960). Factors to be considered "include the nature of the article, the circumstances surrounding the preservation and custody of it, and the **likelihood of intermeddlers tampering with it**." *Gallego*, at 917. *State v. Campbell*, 691 P. 2d 929 - Wash: Supreme Court 1984 at ¶8. (Emphasis added).

Unmistakable proof of the "likelihood of intermeddlers"

As discussed above, Petitioner has shown by substantial evidence that a "likelihood of intermeddlers" exists in the current voting system in its inability to preserve an unbroken chain of bipartisan custody.

The current election practices are markedly out of synch with the statutes. The system is highly vulnerable to "intermeddlers" and therefore does not insure an unbroken bipartisan chain of custody. Remarkably, mail-in ballots are not counted by a bipartisan group in each county, external to "any machines", or verified in any non-machine statistical bi-partisan human observable manner, which should then hand deliver the vote tallies to the State tabulator in order to maintain an unbroken chain of custody.

CONCLUSION & REMEDIES

The voting process must enable an unbroken bipartisan chain of custody.

Therefore, the citizens of the State of Washington have no adequate remedy for the incurable uncertainty that exists currently in the current voting system. Therefore, Petitioner requests that the Secretary of State immediately:

(1) Stop all involvement by Microsoft, at least until their involvement can be assessed and certified as honest by a properly constituted bipartisan group;

(2) Verify the identity and qualification of each person who presents themselves to vote through a bipartisan group;

(3) Stop using electronic voting machines immediately;

(4) Establish bipartisan groups at each location where mail-in votes are counted. (How identities are confirmed is highly suspect with mail-in. Voters need to

physically show up to vote and have their thumbs inked unless they are unable to for legitimate reasons);

(5) Implement the process by which the bipartisan group vets each voter for his or her authority to vote;

(6) Enable each bipartisan group to count each verified ballot and prepare a tally sheet that will be certified by the bipartisan group;

(7) Enable the bipartisan group to photograph and post the certified tally sheet on the county‘s website immediately upon the certification;

(8) Provide the address and directions for the bipartisan group to drive to the state tabulator to report their tally sheet; and

(9) Enable the bipartisan group to be able to verify that their tally sheet results are faithfully entered into the State tabulator.

Respectfully submitted,

/S/ James M. Miller

James M Miller, Citizen Petitioner
1 Blue Sky Place
Omak, WA 98841
(425) 471-8101
jmiller@leader.com

August 6, 2018

VERIFICATION

I, James M. Miller, being of sound mind and body do hereby affirm that information in this writ is true and accurate to the best of my knowledge and ability, including my attestations as a process control expert. *See* **Exhibit L**.

/S/ James M. Miller

_____

James M. Miller

/S/ Notary Signature & Stamp on File

SWORN AND SUBSCRIBED before me, a Notary Public, this ____ day of _____, 2018.

VERIFICATION

I, James M. Miller, being of sound mind and body do hereby affirm that information in this writ is true and accurate to the best of my knowledge and ability, including my attestations as a process control expert.

James M. Miller

James M. Miller

SWORN AND SUBSCRIBED before me, a Notary Public, this 6 day of August, 2018.

Gay L. Heindselman
8/6/2018

SUPERIOR COURT
OKANOGAN COUNTY

CERTIFICATE OF SERVICE

I, James M. Miller, hereby certify that on August 6, 2018 a true and accurate copy of the foregoing WRIT OF MANDAMUS was served upon the Washington Secretary of State's designated service officer Brenda Galarza, Records/Public Disclosure Officer, Office of the Secretary of State Kim Wyman, 801 Capital Way South, Olympia, Washington 98501, (360) 704-5220, brenda.galarza@sos.wa.gov.

/S/ James M. Miller

James M Miller, Citizen Petitioner
1 Blue Sky Place
Omak, WA 98841
(425) 471-8101
jmiller@leader.com

August 6, 2018

Exhibit A

Laurie Thomas. (Jun. 8, 2018). James Miller signed response 6-8-18001.
Okanogan County Auditor.

Okanogan County Auditor

Laurie Thomas, Auditor *Mila Jury, Chief Deputy Auditor*
PO Box 1010
Okanogan WA 98840
509-422-7240

June 7, 2018

James M. Miller
1 Blue Sky Pl
Omak, WA 98841

Dear Mr. Miller,

As I understand it your request was for the entire "election process manual". To fulfill this request I am attaching the "desk reference" instructions compiled and utilized by Okanogan County staff.

A few "screen shots" have been redacted from the instructions due to the inclusion of security passwords, passcodes and other security sensitive information exempt from disclosure under RCW 42.56.420(4).

We are also withholding proprietary information, including specific instruction manuals for HART and VOTEC at the instruction of the vendors we contract with because their documents are exempt from disclosure under the Public Records Act. RCW 42.56.270.
If you should disagree about the applicability of the "financial, commercial, and proprietary information" exemption, then the companies that created the records can set the matter for a court hearing and ask for a declaration from the court that the exemption applies, and an injunction preventing disclosure.

Please consider this response for records as defined in RCW 42.56.010(3) timely pursuant to the requirements of RCW 42.56. I believe this fulfills your request and will consider this matter closed. If you object to any withholding of records you must follow the administrative procedures described in Okanogan County Code 2.88.070 before seeking judicial review. Feel free to contact this office if you require further assistance in this matter.

Cordially,

Laurie Thomas

Laurie Thomas, Auditor

Exhibit B

Brenda Galarza. (Jun. 29, 2018). PDR #18H-165 Public Records request for electronic voting procedures. Office of the WA Secretary of State, Elections Division.

RE: RE: PDR #18H-165 Public Records request for electronic votingprocedures

From: Holmes, Stuart <stuart.holmes@sos.wa.gov>
Sent: Fri, Jun 29, 2018 at 3:14 pm
To: Jim Miller, Galarza, Brenda
Cc: Condotta, Rep. Cary, mike.steele@leg.wa.gov, brad.hawkins@leg.wa.gov, Kretz Joel

image001.png (30.2 KB) image002.jpg (5.3 KB) image003.jpg (7.9 KB) image004.png (10.3 KB) image005.png (10.3 KB) – **Download all**

Jim,

Happy to answer your questions. Additionally, in the State of Washington a paper ballot is required by law. Each and every voter's ballot has a voter-

1. Please provide the list of vendors of voting machines used in the state election process for each county?
   a. A list of voting equipment used by each county is available on our website here: https://www.sos.wa.gov/elections/research/voting

2. Specifically name the 3rd party testers and how they are certified, and how they maintain unbroken bipartisan chain of custody if bipartisar in person and then creating a report based on 'empirical observable phenomena? this question was not answered.
   a. According to the Election Assistance Commission (EAC) website, SLI Compliance, a Division of Gaming Laboratories International, LL
   b. For more information about how they become accredited please refer to the EAC's website: https://www.eac.gov/voting-equipmen
   c. Additionally, you can review all the testing documentation on the EAC's website here: https://www.eac.gov/voting-equipment/syste

4. Please provide the public record that states that multi-partisan chain of custody of ballots and tally totals is maintained, and is 'never secret then, by the Grace of God.
   a. As I mentioned before, it is required that counties use numbered seals and logs, or other security measures which will detect any in materials and must be accompanied by at least two county auditor staff at all times. (WAC 434-261-045, WAC 434-250-110 & RCW 2 retention schedule. (https://www.sos.wa.gov/_assets/archives/county-auditor-rrs-ver-5.0.pdf). The Secretary of State's Office doesn custody' documents. However, you could certain view or get more information about those documents from each county auditor.
   b. Ballots are also maintained according to the retention schedule. (https://www.sos.wa.gov/_assets/archives/county-auditor-rrs-ver-5
   c. Audits are observable by the public and required to be conducted prior to the certification of each election. Logic and Accuracy test 29A.60.170, WAC 434-335-240 & RCW 29A.12.130).

Stuart Holmes| Voting Information Systems Manager
Office of the Secretary of State
(360) 725-5794 | www.vote.wa.gov

Office of the Secretary of State
Elections Division

From: Jim Miller [mailto:jimomak@leader.com]
Sent: Friday, June 29, 2018 2:39 PM
To: Holmes, Stuart <stuart.holmes@sos.wa.gov>; Galarza, Brenda <brenda.galarza@sos.wa.gov>
Cc: Condotta, Rep. Cary <cary.condotta@leg.wa.gov>; mike.steele@leg.wa.gov; brad.hawkins@leg.wa.gov; Kretz Joel <kretzranch@gmail.com>
Subject: RE: RE: PDR #18H-165 Public Records request for electronic voting procedures

Public Records Request of the following:
1. Please provide the list of vendors of voting machines used in the state election process for each county?

2. Specifically name the 3rd party testers and how they are certified, and how they maintain unbroken bipartisan chain of cus present to witness such testing in person and then creating a report based on 'empirical observable phenomena? this questi

4. Please provide the public record that states that multi-partisan chain of custody of ballots and tally totals is maintained, an will go away, and not until then, by the Grace of God.

I cannot accept that multi-partisan chain of custody can be maintained in 'any computer system'. Citizens 'cannot' observe s chain of custody is not maintained, and by law...the election process is by logic invalid. We simply MUST perform elections w custody. Ballot tallies must 'never' go to 'silicon' because they are then 'hidden and secret'.

-----Original Message-----
From: "Holmes, Stuart" <stuart.holmes@sos.wa.gov>
Sent: Friday, June 29, 2018 9:47am
To: "Jim Miller" <jimomak@leader.com>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

Jim,

First, thank you for reaching out to our office with you questions. I just want to make it clear that not Smartmatic voting system or equipment is not

1. specifically name the 3rd party tester (and the actually testers themselves) and how that company and those people are certified by a bipar
    a. Independent testing authorities (or commonly known as Voting System Testing Laboratories (VSTL)) are designated by the United St
2. When the memory stick is delivered to the county auditor by the vendor what 'proof exists', other than a 'certification piece of paper' that t
    a. County Auditors are required to do acceptance testing of their voting system prior to use as well as Logic and Accuracy Testing of th system, including hardware and software, is the certified voting system. Each voting system can produce a hash value that would cor Laboratory. This hash value would show that the software in use has not been changed. (WAC 434-335-240 & RCW 29A.12.130). Log observers.
3. Is the 'memory stick, on which the tally at each county is entered and sent to the state, tested against an encrypted part number sent to the such as certified mail to ensure that the proper 'memory stick' has been delivered to the auditor by comparison(a phone call recorded)?
    a. If the 'memory stick' is part of the voting system, then yes that can be done. However, not all voting systems have 'memory sticks' a method they'd like to transfer election results from the tabulation system. For example, some counties use one-write media like CDs formatted prior to use. In either case, they are secured before and after the election.
4. What programs exist on the memory stick?
    a. None. They are only used to transfer files in some counties depending on the voting system and procedures in place for that county
5. What circuits exist on the memory stick, and what circuits are 'blue printed' as the baseline as the 'official circuits', and how is this tested ar
    a. This would be county specific based on the 'memory sticks' in use for the voting system and procedures in place for that county.
6. Are the 'memory sticks' impounded after the election, and are they available for inspection after the election and for how long, or is the evi
    a. This is county specific depending on the voting system and procedures in place for that county because not all counties use the sam related to the election have a retention and must be retained for their entire retention period. (https://www.sos.wa.gov/_assets/arc
7. Is there a 'micro-voltage' activation 'count' embedded in the memory stick's program, so that when it is received at the county auditor's site been reprogrammed during 'transport', by a 'man in the middle'? (this would make the whole voting procedure a magic act as it exists)
    a. Election Results are verified using a paper copy of the results. When results are transported from the tabulation equipment to be u the results are appearing accurately. Additionally, that same paper copy is provided to the state to ensure that after the results were several methods and opportunities, as stated in our previous response, for auditing during the election canvassing to ensure the tab
8. Is each county auditor required to create a 'bipartisan human hand tally' as well as a PCOS/Smartmatic machine tally to audit each 'tally cou unbroken bipartisan chain of custody tallies?
    a. Smartmatic voting systems are not certified or used in the State of Washington.

Stuart Holmes| Voting Information Systems Manager
Office of the Secretary of State
(360) 725-5794 | www.vote.wa.gov

Office of the Secretary of State
Elections Division

From: Galarza, Brenda
Sent: Friday, June 29, 2018 9:39 AM
To: Jim Miller <jimomak@leader.com>
Cc: Holmes, Stuart <stuart.holmes@sos.wa.gov>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

Mr. Miller,

Washington State follows the Public Records Act RCW 42.56. FOIA is for federal records request. Your questions do not constitute a records request Stuart Holmes. He will respond to your additional questions.

Regards,

Brenda Galarza
Records/Public Disclosure Officer
360-704-5220
Office of the Secretary of State
Kim Wyman

From: Jim Miller [mailto:jimomak@leader.com]
Sent: Friday, June 29, 2018 9:15 AM
To: Galarza, Brenda <brenda.galarza@sos.wa.gov>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

I do have additional questions, as I have not received satisfactory or conclusive evidence that bipartisan chain of custody is p electronic devices of any kind in WA state's voting process. It is the 'people's' responsibility to ensure unbroken bipartisan ch under the Federal and the WA state constitution to know that this is true. We are not stating that there is 'voter fraud', we are is in reality—not broken beyond a 'shadow of doubt'. Any action taken, whereby the 'tally' or 'counts' of any voting procedure a when it is performed and transmitted by 'electrons' in a 'digital form' fails the test of 'unbroken bipartisan chain of custody obs bipartisan chain of custody be subject to 'FAITH' , 'law', 'vendor certification', testing' or any process' that is 'hidden from emp 'certification', it by logic, and physical law fails the test. The will of the people cannot be subject 'FAITH' from government, the without failure. Electronic devices depend upon 'failure modes' or 'statistical outcomes' that depend upon 'software programs which are 'hidden from observation, and thus fail the test by default of logic of 'unbroken bipartisan chain of custody'. Thus, t the test for certification. It is open to 'man in the middle attacks', and corruption. As such, the 'will of the people' can be circur through electronic means. This is the underlying logic of my FOIA requests.

FOIA request question:
1. specifically name the 3rd party tester (and the actually testers themselves) and how that company and those people are c WA?
2. When the memory stick is delivered to the county auditor by the vendor what 'proof exists', other than a 'certification piece delivered'?
3. Is the 'memory stick, on which the tally at each county is entered and sent to the state, tested against an encrypted part nu communication channel such as certified mail to ensure that the proper 'memory stick' has been delivered to the auditor by c
4. What programs exist on the memory stick?
5. What circuits exist on the memory stick, and what circuits are 'blue printed' as the baseline as the 'official circuits', and how
6. Are the 'memory sticks' impounded after the election, and are they available for inspection after the election and for how lo
7. Is there a 'micro-voltage' activation 'count' embedded in the memory stick's program, so that when it is received at the cou to attest that it has not been reprogrammed during 'transport', by a 'man in the middle'? (this would make the whole voting pr
8. Is each county auditor required to create a 'bipartisan human hand tally' as well as a PCOS/Smartmatic machine tally to a preserving both tally counts as unbroken bipartisan chain of custody tallies?

Please provide the public records for these questions as a continuance of the original FOIA request as noted by your statem

——Original Message——
From: "Galarza, Brenda" <brenda.galarza@sos.wa.gov>
Sent: Thursday, June 28, 2018 11:16am
To: "jimomak@leader.com" <jimomak@leader.com>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

Mr. Miller,

Below is information provided by our Elections Division.

1. How do you ensure bi-partisan 'chain of custody' on any electronic device that sits between the voter and the 'county/city/special district' for loca election' for federal positions?

> To answer your question, I'm interpreting "electronic device" as an in-person ballot marking system that retains an electronic voting record machine, and the county's voting system that tabulates returned ballots.

Before any voting system can be used in the State of Washington it first must be tested and certified by an independent testing authority de: well as inspected and tested by the Secretary of State's Office (RCW 29A.12.080). During the Secretary of State's inspection of the voting syst (WAC 434-335-040) which include "Secures to the voter secrecy in the act of voting" and "Be capable of being secured with lock and seal wh

The Secretary of State's Office requires the use of secure storage which must employ the use of numbered seals and logs, or other security n access to the secured ballot materials and must be accompanied by at least two county auditor staff at all times. (WAC 434-261-045, WAC 43 used by every county document the chain of custody for who accessed the secured ballots which includes electronic voting devices that reta certification requirements of any voting system is that the voting device must produce a voter verifiable paper ballot.

Additionally, observers may be present during the processing of ballots because the entire process is open to the public.

2. How do you ensure that the 'electronic devices' are monitored by 'bipartisan' citizens, trained to monitor the ballot tally totals?

Prior to each election, the County Auditor must request observers be appointed by the major political parties to be present during the proce requested to appoint observers. The County Auditor can train observers with respect to ballot processing procedures and the vote tallying sy

3. do you ensure the bipartisan election monitors/judges can affirmatively verify that each vote is entered, reported, and tallied without interventio be empirically observable?

Prior to certification of the election the County Auditor must audit of results of votes cast on any direct recording electronic voting devices u counting equipment, and an audit of duplicated ballots.

In 2019, Risk Limiting Audits will become an option for counties to use to audit their voting equipment. Rules for conducting a Risk Limiting A Audits provide statistical evidence and confidence that the count was accurate while keeping the resources needed by the county to as little

4. I request the 'public records' that prove the above questions regarding the usage of all 'electronic devices' used in the voting process...all stages w of the voting procedure that results in a 'summation', 'addition', 'subtraction', 'tally', 'vote count' as an 'official' record of the voting process.

If you're interested in the chain of custody logs, observer procedures, audit procedures, or specific documents about the use of the voting sy Auditor because the Secretary of State's Office does not process any ballots, conduct tabulation, or operate a voting system.

If you're interested in the Election Assistance Commission testing and certification of the voting systems, those test reports and certification equipment/system-certification-process-s/

We also have information about the system in use in Washington on our website here: https://www.sos.wa.gov/elections/research/voting-s

I trust you will find this information useful. If you have any further questions, please let me know. Otherwise, I am closing this request today.

Regards,

Brenda Galarza
Records/Public Disclosure Officer
PO Box 40224 | Olympia, WA 98504-0224
360-704-5220 Phone | 360-704-7830 Fax
brenda.galarza@sos.wa.gov

Office of the Secretary of State
Kim Wyman

From: Jim Miller [mailto:jlmomak@leader.com]
Sent: Friday, June 22, 2018 10:46 AM
To: Galarza, Brenda <brenda.galarza@sos.wa.gov>
Cc: bhires@omakchronicle.com; Condotta, Rep. Cary <cary.condotta@leg.wa.gov>; mike.steele@leg.wa.gov; brad.hawkins@leg.wa.gov
Subject: FW: RE: PDR #18H-165 FOIA request for electronic voting procedures

Please consider this a FOIA request with the questions as stated:

1. How do you ensure bi-partisan 'chain of custody' on any electronic device that sits between the voter and the 'county/city/s state elections, and the 'federal election' for federal positions?

2. How do you ensure that the 'electronic devices' are monitored by 'bipartisan' citizens, trained to monitor the ballot tally tot

3. do you ensure the bipartisan election monitors/judges can affirmatively verify that each vote is entered, reported, and tallie whose operations do not appear to be empirically observable?

4. I request the 'public records' that prove the above questions regarding the usage of all 'electronic devices' used in the voti any manner by non-humans, as part of the voting procedure that results in a 'summation','addition', 'subtraction', 'tally', 'vote

-----Original Message-----
From: "Public Records, House" <House.PublicRecords@leg.wa.gov>
Sent: Friday, June 22, 2018 10:19am
To: "Jim Miller" <jimomak@leader.com>
Cc: "Public Records, Senate" <Senate.PublicRecords@leg.wa.gov>, "Condotta, Rep. Cary" <Cary.Condotta@leg.wa.gov>, "
"Hawkins, Sen. Brad" <Brad.Hawkins@leg.wa.gov>
Subject: RE: PDR #18H-165

Dear Mr. Miller:

I understand you are requesting "documentation of the processes utilized statewide at each county, including confidential sof utilized in the election process". If this is correct, then you will need to direct your request to the Public Records Officer for th

If you have any questions, please let me know.

Thank you,

Samina M. Mays
Public Records Officer
Washington State House of Representatives
360.786.7227 | Samina.Mays@leg.wa.gov

From: Jim Miller <jimomak@leader.com>
Sent: Thursday, June 21, 2018 4:28 PM
To: Public Records, House <House.PublicRecords@leg.wa.gov>
Cc: Public Records, Senate <Senate.PublicRecords@leg.wa.gov>; Condotta, Rep. Cary <Cary.Condotta@leg.wa.gov>; Steele, Rep. Mike <Mike.Steele@
Subject: RE: PDR #18H-165

What we have in play is a 'catch-22'. My FOIA request is for 'information' that exists as a public record, most likely as an 'elec designation', which makes it 'hidden and secret', and thus not a 'public record' by definition. So, by definition, what the voters not available, to the voters. What a perfect legal 'black box' behind which to hide.

Therefore, I must conclude, that the 'election process', in total, has 'no bipartisan chain of custody' which can be viewed by th 'certified' when chain of custody cannot be proven, and the Secretary of State, by law cannot 'certify' that which is 'secret anc

If we cannot view that which is hidden and secret, then we have no recourse but to serve to the state an injunction to stop th can be replace with an 'open and honest' election process from registration to tally count total, such that the 'will of the peopl election. What this means, is that, in the end, no electronic machines of any type can be utilized in the voting process.

This is a FOIA request, to provide the documentation of the processes utilized statewide at each county, including confidentia utilized in the election process.

-----Original Message-----
From: "Public Records, House" <House.PublicRecords@leg.wa.gov>

Sent: Thursday, June 21, 2018 10:35am
To: "jimomak@leader.com" <jimomak@leader.com>
Cc: "Public Records, Senate" <Senate.PublicRecords@leg.wa.gov>
Subject: PDR #18H-165

Dear Mr. Miller:

As the records custodian for the House of Representatives, the Office of the Chief Clerk has received your FOIA request for Representati have assigned your request tracking number 18H-165. Please put this number on all future correspondence regarding this request.

You requested the following information:
How do you ensure bi-partisan 'chain of custody' on any electronic device that sits between the voter and the 'county/city/special district the 'federal election' for federal positions?
How do you ensure that the 'electronic devices' are monitored by 'bipartisan' citizens, trained to monitor the ballot tally totals?
How do you ensure the bipartisan election monitors/judges can affirmatively verify that each vote is entered, reported, and tallied withou do not appear to be empirically observable?

It appears that your request is for information only and not for an "identifiable record" under the Public Records Act (RCW 42.56.080, ar so I can help identify which records you wish to obtain. I will now consider this request closed. Please contact me if you have any questic

Thank you,

Samina M. Mays
Public Records Officer
Washington State House of Representatives
360.786.7227 | Samina.Mays@leg.wa.gov

Your email security and privacy matter.

Your email security and privacy matter.

Your email security and privacy matter.

Exhibit C

Ron Wyden et al. (Jun. 12, 2018). Proposed Amendment to the Help America Vote Act of 2002. 115th Congress, 2d Session. U.S. Senate.

115TH CONGRESS
2D SESSION

S. _____

To amend the Help America Vote Act of 2002 to require paper ballots and risk limiting audits in all Federal elections, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself, Mrs. GILLIBRAND, Ms. WARREN, Mrs. MURRAY, Mr. MARKEY, and Mr. MERKLEY) introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To amend the Help America Vote Act of 2002 to require paper ballots and risk limiting audits in all Federal elections, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protecting American Votes and Elections Act of 2018".

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) Access to the ballot, free and fair elections, and a trustworthy election process are at the core of

American Democracy. Just as the Founding Fathers signed their names to paper supporting their views for a government by and for the people, access to the paper ballot is the best way to ensure elections stay by and for the American people. Using paper provides an easily auditable, tamper proof, and simple way for citizens to access their ballot. It is for these reasons and more that using paper ballots to ensure resilient and fair elections should be the priority of this Nation.

(2) Risk-limiting audits will help to protect our elections from cyberattacks, by ensuring that if the electoral outcome is incorrect, for instance because someone tampered with the electronic counts or reporting, the audit has a large, known probability of correcting the outcome by requiring a full hand count. Paper ballots are vital to the audit process since, other than through manual inspection of a sample of paper ballots, there is currently no reliable way to determine whether an election was hacked or the outcome was miscalculated.

(3) Risk-limiting audits are a cost effective way of auditing election results. They generally require inspecting only a small percentage of the ballots cast in an election, and proceed to a full hand count only

when sampling does not provide strong evidence that the reported outcome is correct. This will ensure that Americans have confidence in their election results, without the cost of a full recount of every ballot in the country.

SEC. 3. PAPER BALLOT AND MANUAL COUNTING REQUIREMENTS.

(a) IN GENERAL.—Section 301(a)(2) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(2)) is amended to read as follows:

"(2) PAPER BALLOT REQUIREMENT.—

"(A) VOTER-VERIFIED PAPER BALLOTS.—

"(i) PAPER BALLOT REQUIREMENT.—

(I) The voting system shall require the use of an individual, durable, voter-verified, paper ballot of the voter's vote that shall be marked and made available for inspection and verification by the voter before the voter's vote is cast and counted, and which shall be counted by hand or read by an optical character recognition device or other counting device. For purposes of this subclause, the term 'individual, durable, voter-verified, paper ballot' means a paper ballot marked by the voter by hand or a

paper ballot marked through the use of a nontabulating ballot marking device or system, so long as the voter shall have the option to mark his or her ballot by hand.

"(II) The voting system shall provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved in accordance with clause (ii).

"(III) The voting system shall not preserve the voter-verified paper ballots in any manner that makes it possible, at any time after the ballot has been cast, to associate a voter with the record of the voter's vote without the voter's consent.

"(ii) PRESERVATION AS OFFICIAL RECORD.—The individual, durable, voter-verified, paper ballot used in accordance with clause (i) shall constitute the official ballot and shall be preserved and used as the official ballot for purposes of any recount or audit conducted with respect to any election for Federal office in which the voting system is used.

"(iii) MANUAL COUNTING REQUIREMENTS FOR RECOUNTS AND AUDITS.—(I) Each paper ballot used pursuant to clause (i) shall be suitable for a manual audit, and shall be counted by hand in any recount or audit conducted with respect to any election for Federal office.

"(II) In the event of any inconsistencies or irregularities between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified, paper ballots used pursuant to clause (i), and subject to subparagraph (B), the individual, durable, voter-verified, paper ballots shall be the true and correct record of the votes cast.

"(iv) APPLICATION TO ALL BALLOTS.—The requirements of this subparagraph shall apply to all ballots cast in elections for Federal office, including ballots cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act and other absentee voters.

"(B) SPECIAL RULE FOR TREATMENT OF DISPUTES WHEN PAPER BALLOTS HAVE BEEN SHOWN TO BE COMPROMISED.—

"(i) IN GENERAL.—In the event that—

"(I) there is any inconsistency between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified, paper ballots used pursuant to subparagraph (A)(i) with respect to any election for Federal office; and

"(II) it is demonstrated by clear and convincing evidence (as determined in accordance with the applicable standards in the jurisdiction involved) in any recount, audit, or contest of the result of the election that the paper ballots have been compromised (by damage or mischief or otherwise) and that a sufficient number of the ballots have been so compromised that the result of the election could be changed,

the determination of the appropriate remedy with respect to the election shall be made in accordance with applicable State law, except that the electronic tally shall not be used as the exclusive basis for determining the official certified result.

"(ii) RULE FOR CONSIDERATION OF BALLOTS ASSOCIATED WITH EACH VOTING MACHINE.—For purposes of clause (i), only the paper ballots deemed compromised, if any, shall be considered in the calculation of whether or not the result of the election could be changed due to the compromised paper ballots.".

(b) CONFORMING AMENDMENT CLARIFYING APPLICABILITY OF ALTERNATIVE LANGUAGE ACCESSIBILITY.—Section 301(a)(4) of such Act (52 U.S.C. 21081(a)(4)) is amended by inserting "(including the paper ballots required to be used under paragraph (2))" after "voting system".

(c) OTHER CONFORMING AMENDMENTS.—Section 301(a)(1) of such Act (52 U.S.C. 21081(a)(1)) is amended—

(1) in subparagraph (A)(i), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)";

(2) in subparagraph (A)(ii), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)";

(3) in subparagraph (A)(iii), by striking "counted" each place it appears and inserting "counted, in accordance with paragraphs (2) and (3)"; and

(4) in subparagraph (B)(ii), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)".

(d) EFFECTIVE DATE.—Notwithstanding section 301(d) of the Help America Vote Act of 2002 (52 U.S.C. 21081(d)), each State and jurisdiction shall be required to comply with the amendments made by this section for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.

SEC. 4. ACCESSIBILITY AND BALLOT VERIFICATION FOR INDIVIDUALS WITH DISABILITIES.

(a) IN GENERAL.—Section 301(a)(3)(B) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(3)(B)) is amended to read as follows:

"(B)(i) satisfy the requirement of subparagraph (A) through the use of at least 1 voting system equipped for individuals with disabilities, including nonvisual and enhanced visual accessibility for the blind and visually impaired, and nonmanual and enhanced manual accessibility for the mobility and dexterity impaired, at each polling place; and

"(ii) meet the requirements of subparagraph (A) and paragraph (2)(A) by using a system that—

"(I) allows the voter to privately and independently verify the permanent paper ballot through the presentation, in accessible form, of the printed or marked vote selections from the same printed or marked information that would be used for any vote counting or auditing; and

"(II) allows the voter to privately and independently verify and cast the permanent paper ballot without requiring the voter to manually handle the paper ballot; and".

(b) SPECIFIC REQUIREMENT OF STUDY, TESTING, AND DEVELOPMENT OF ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.—

(1) STUDY AND REPORTING.—Subtitle C of title II of such Act (52 U.S.C. 21081 et seq.) is amended by inserting after section 246 the following new section:

"SEC. 246A. STUDY AND REPORT ON ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.

"(a) STUDY AND REPORT.—The Director of the National Science Foundation shall make grants to not fewer than 3 eligible entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms and devices and best practices to enhance the accessibility of paper ballot voting and verification mechanisms for individuals with disabilities, for voters whose primary language is not English, and for voters with difficulties in literacy, including best practices for the mechanisms themselves and the processes through which the mechanisms are used.

"(b) ELIGIBILITY.—An entity is eligible to receive a grant under this part if it submits to the Director (at such time and in such form as the Director may require) an application containing—

"(1) certifications that the entity shall specifically investigate enhanced methods or devices, including non-electronic devices, that will assist such individuals and voters in marking voter-verified paper ballots and presenting or transmitting the information printed or marked on such ballots back to such individuals and voters, and casting such ballots;

"(2) a certification that the entity shall complete the activities carried out with the grant not later than December 31, 2020; and

"(3) such other information and certifications as the Director may require.

"(c) AVAILABILITY OF TECHNOLOGY.—Any technology developed with the grants made under this section shall be treated as non-proprietary and shall be made available to the public, including to manufacturers of voting systems.

"(d) COORDINATION WITH GRANTS FOR TECHNOLOGY IMPROVEMENTS.—The Director shall carry out this section so that the activities carried out with the grants made under subsection (a) are coordinated with the research conducted under the grant program carried out by the Commission under section 271, to the extent that the Director and Commission determine necessary to provide for the advancement of accessible voting technology.

"(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out subsection (a) $10,000,000, to remain available until expended.".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by inserting after the item relating to section 246 the following new item:

"Sec. 246A. Study and report on accessible paper ballot verification mechanisms.".

SEC. 5. RISK-LIMITING AUDITS.

(a) IN GENERAL.—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended by inserting after section 303 the following new section:

"SEC. 303A. RISK-LIMITING AUDITS.

"(a) DEFINITIONS.—In this section:

"(1) RISK-LIMITING AUDIT.—

"(A) IN GENERAL.—The term 'risk-limiting audit' means a post-election process such that, if the reported outcome of the contest is incorrect, there is at least a 95 percent chance that the audit will replace the incorrect outcome with the correct outcome as determined by a full, hand-to-eye tabulation of all votes validly cast in that election contest that ascertains voter intent manually and directly from voter-verifiable paper records.

"(B) REPORTED OUTCOME.—The term 'reported outcome' means the outcome of an election contest which is determined according to the canvass and which will become the official, certified outcome unless it is revised by an audit, recount, or other legal process.

"(C) INCORRECT OUTCOME.—The term 'incorrect outcome' means an outcome that differs from the outcome that would be determined by a full tabulation of all votes validly cast in that election contest, determining voter intent manually, directly from voter-verifiable paper records.

"(D) OUTCOME.—The term 'outcome' means the winner or set of winners of an election contest, which might be candidates or positions.

"(2) BALLOT MANIFEST.—The term 'ballot manifest' means a record maintained by each county that—

"(A) is created without reliance on any part of the voting system used to tabulate votes;

"(B) functions as a sampling frame for conducting a risk-limiting audit; and

"(C) contains the following information about ballots cast and counted:

"(i) The total number of ballots cast and counted in the election (including undervotes, overvotes, and other invalid votes).

"(ii) The total number of ballots cast in each contest in the election (including undervotes, overvotes, and other invalid votes).

"(iii) A precise description of the manner in which the ballots are physically stored, including the total number of physical groups of ballots, the numbering system for each group, a unique label for each group, and the number of ballots in each such group.

"(b) REQUIREMENT.—

"(1) IN GENERAL.—

"(A) AUDITS.—Each State and jurisdiction shall administer risk-limiting audits of the results of all elections for Federal office held in the State in accordance with the requirements of paragraph (2).

"(B) FULL MANUAL TALLY.—If a risk-limiting audit conducted under subparagraph (A) leads to a full manual tally of an election contest, the State or jurisdiction shall use the results of the full manual tally as the official results of the election contest.

"(2) AUDIT REQUIREMENTS.—

"(A) RULES AND PROCEDURES.—

"(i) IN GENERAL.—Risk-limiting audits shall be conducted in accordance with the rules and procedures established by the chief State election official of the State not later than 1 year after the date of the enactment of this section.

"(ii) MATTERS INCLUDED.—The rules and procedures established under clause (i) may include the following:

"(I) Rules for ensuring the security of ballots and documenting that prescribed procedures were followed.

"(II) Rules and procedures for ensuring the accuracy of ballot manifests produced by jurisdictions.

"(III) Rules and procedures for governing the format of ballot mani-

fests, cast vote records, and other data involved in risk-limiting audits.

"(IV) Methods to ensure that any cast vote records used in a risk-limiting audit are those used by the voting system to tally the election results sent to the Secretary of State and made public.

"(V) Procedures for the random selection of ballots to be inspected manually during each audit.

"(VI) Rules for the calculations and other methods to be used in the audit and to determine whether and when the audit of each contest is complete.

"(VII) Procedures and requirements for testing any software used to conduct risk-limiting audits.

"(B) TIMING.—The risk-limiting audit shall be completed not later than the date that the result of the election is certified by the State.

"(C) PUBLIC REPORT.—After the completion of the risk-limiting audit, the State shall

publish a report on the results of the audit, together with such information as necessary to confirm that the audit was conducted properly.

"(c) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this section for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.".

(b) CONFORMING AMENDMENTS RELATED TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111) is amended by striking "and 303" and inserting "303, and 303A".

(c) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 303 the following new item:

"Sec. 303A. Risk-limiting audits.".

Exhibit D

Jay Inslee. (Jul. 19, 2018). Letter to President Donald Trump. WA State Governor's Office.

July 19, 2018

President Donald. J. Trump
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear President Trump:

We write with complete and total dismay and alarm over your comments at the summit with Russian President Vladimir Putin and your failure to both recognize and denounce his attacks on American democracy. Never, in the course of our nation's history, has a president sided with a foreign adversary—one responsible for a coordinated attack on our free and open elections—over our own U.S. intelligence community.

We now know, unequivocally, that—on the order of President Putin—Russian officials attacked at least 21 state systems during the 2016 election, as part of a coordinated effort to influence our elections. Last week, FBI special counsel Robert Mueller indicted twelve Russian intelligence officers accused of interfering in the 2016 election. The U.S. intelligence community confirmed these facts in no uncertain terms. Your inconsistency in accepting those facts, and your inability to confront President Putin, poses a direct threat to our national security and to our freedoms.

Our election systems remain targets of foreign interference. On February 13, 2018, Director of National Intelligence Dan Coats, testifying before the Senate Intelligence Committee, said that "persistent and disruptive cyber operations" would continue "using elections as opportunities to undermine democracy" in the United States in 2018 and beyond. In that same hearing, he affirmed that he had already seen evidence Russia was targeting U.S. elections in November 2018.

As governors, we remain committed to protecting our states' election systems. There is nothing more fundamental to the enduring success of our American democracy, and we take seriously our responsibility to protect the integrity and security of our elections. Through the National Governors Association and public-private partnerships, we have led a number of bipartisan initiatives on cybersecurity to bolster the security of our election infrastructure. States are leading the way in protecting voters, but more has to be done to send a clear message: Interference in our elections will not be tolerated.

We cannot take a passive stance while a hostile foreign government continues to undermine our democracy. And we certainly cannot defend or actively condone Russia's actions, which is what you are choosing to do. Ignoring the real threats Russia poses to our elections is, quite frankly, un-American. This is an imminent national security threat that transcends party lines. This is a matter of protecting and preserving fair elections—the underpinning of our democracy.

As governors, we are committed to ensuring that every vote is protected and counted. Americans need a president who is willing to stand-up to a foreign adversary that continues to threaten our basic rights and freedom.

We call on you to stand with the American people and lead by denouncing the Russian government's assault on the fundamental and basic right of Americans to elect their leaders without interference. We call on you to enforce and strengthen sanctions against Russia and hold them accountable for their continued attacks. Lastly, we call on you to support strong congressional action to help states secure our elections and protect our democracy from Russian cyberattacks. The American people deserve better.

Sincerely,

Jay Inslee
Governor
State of Washington

Andrew Cuomo
Governor
State of New York

Exhibit E

Kim Wyman. (Accessed Aug. 03, 2018). Election Machine Inventory, SOS website. Washington, Secretary of State.

Voting Systems by County					
County	System	Type of AVU*	Vendor	Software	Accessible Voting Unit
Adams	Optical Scan	Touchscreen	Election Systems and Software	EVS	AutoMark
Asotin	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Benton	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Chelan	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Clallam	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Clark	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Columbia	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Cowlitz	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Douglas	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Ferry	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Franklin	Digital Scan	Touchscreen	Dominion Voting Systems	Democracy Suite	AVC Edge
Garfield	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Grant	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Grays Harbor	Digital Scan	Touchsceen	ClearBallot	ClearVote	ClearAccess
Island	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Jefferson	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
King	Digital Scan	Touchscreen	ClearBallot	ClearVote	ClearAccess
Kitsap	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Kittitas	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Klickitat	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Lewis	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Lincoln	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Mason	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Okanogan	Digital Scan	Dial	Hart InterCivic	HVS	eSlate

Pacific	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Pend Oreille	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Pierce	Digital Scan	Touchscreen	ClearBallot	ClearVote	ClearAccess
San Juan	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Skagit	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Skamania	Digital Scan	Touchscreen	ClearVote	ClearVote	ClearAccess
Snohomish	Digital Scan	Touchscreen	ClearVote	ClearVote	ClearAccess
Spokane	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Stevens	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Thurston	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Wahkiakum	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Walla Walla	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Whatcom	Digital Scan	Touchscreen	ClearBallot	ClearVote	ClearAccess
Whitman	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Yakima	Digital Scan	Dial	Hart InterCivic	HVS	eSlate

Exhibit F

Angela Gunn. (Nov. 01, 2006). Who's building the gear that's running the show? Computerworld.

E-voting and voter registration: The vendors

Who's building the gear that's running the show?

By Angela Gunn

Computerworld | NOV 1, 2006 12:00 AM PT

The biggest vendors of e-voting machinery are also among the largest vendors of voter-registration technology. Roughly speaking, there are four significant players in the e-voting market and three in the voter-registration arena. We follow our overview of those seven companies with capsule descriptions of other companies whose technology voters may encounter around the country.

E-VOTING VENDORS: THE MAJORS

Diebold Inc.

Not the largest e-voting vendor but certainly the most controversial, **Diebold** has repeatedly raised hackles with its aggressive responses to computer-security professionals who have demonstrated problems with the company's hardware and software. That's leaving out entirely the ill-advised 2003 promise by Diebold CEO and Republican fund-raiser Walden O'Dell to "[help] Ohio deliver its electoral votes to the president." (O'Dell left Diebold in 2005 amid rumors of securities-fraud litigation and insider trading.)

The company produces the AccuVote line of direct recording electronics (DRE), DRE/VVPAT (voter-verified paper audit trail) and optical scan machines. Diebold machines have figured in two high-profile tests that discovered multiple hardware and software vulnerabilities, and they compare poorly with contemporary Sequoia Voting Systems Inc. units in independent tests undertaken in Alameda, Calif.

As of October, various machines from North Canton, Ohio-based Diebold were certified for use in Alaska, Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, New Hampshire, Ohio, Pennsylvania, Tennessee, Texas, Utah, Vermont, Virginia, Washington, Wisconsin and Wyoming. Massachusetts will evaluate several Diebold machines in the commonwealth's November elections.

Diebold is also involved with voter-registration database systems, having purchased Costa Mesa, Calif.-based Data Information Management Systems in 2003. The company has been criticized for its involvement in this summer's voter-registration controversy in Alabama.

Election Systems & Software Inc.
The world's largest elections company, responsible for half of the e-voting machines in the U.S. ES&S was known as American Information Systems until 1997, when the company merged with Business Records Corp. (BRC). Until 1996, its chairman was Chuck Hagel, who quit to run for and win a U.S. Senate seat for Nebraska. Omaha-based ES&S makes a variety of machines, including DRE, DRE/VVPAT and optical-scan versions. It also offers voter-registration database development services. The company produces the iVotronic line of DRE and DRE/VVPAT machines as well as optical scan units. (As part of its purchase of BRC, ES&S ended up with service responsibility for BRC's Optech optical scan machines; for antitrust-related reasons, however, new Optechs come from Sequoia.)

As of October, various machines from **ES&S** were certified for use in Alabama, Arizona, Arkansas, California, Colorado, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Virginia, Washington, West Virginia, Wisconsin and Wyoming. Massachusetts will evaluate several of the company's machines in its November elections.

Hart InterCivic Inc.
Hart InterCivic's Web site nods at the continuing controversy over e-voting technology, promising to "guarantee the best election you've never heard of." (Presumably, that was written before the name-truncation bugs spotted in Virginia and Texas late in the election cycle.) Hart's eSlate machines, unlike most of the competition's units, function essentially as dumb terminals. The user interface is distinguished by the Select Wheel positioning device, which eliminates the use of touch screens. eSlates are available in DRE and DRE/VVPATmodels.

As of October, various machines from Austin-based Hart InterCivic were certified for use in California, Colorado, Hawaii, Illinois, Kentucky, Pennsylvania, Tennessee, Texas, Virginia and Washington. Massachusetts will evaluate several Hart machines in its November elections. Hart is also involved with voter-registration database systems in conjunction with IBM.

Sequoia Voting Systems Inc.
By late October, Oakland, Calif.-based **Sequoia Voting Systems** was once again fending off rumors that the company has connections to the **Venezuelan government**. According to information on the company's Web site, Sequoia's parent company, Smartmatic Corp., is privately owned, with a controlling interest held by founder and CEO Antonio Mugica. Mugica holds dual Spanish and Venezuelan citizenship. Sequoia offers AVC Edge and AVC Advantage DRE units, an AVC Edge DRE/VVPAT unit, and sells a Sequoia-branded Optech Insight optical scanner. (Election Systems & Software also offers an Optech line for reasons explained in the ES&S section.) Also in October, Sequoia figured at the center of tests on Alameda County, Calif., e-voting machines; results (**download PDF**) were generally positive compared with those for a contemporary Diebold unit, though the need for stronger network security and better

handling procedures was emphasized.

As of October, various machines from Sequoia were certified for use in Arizona, California, Colorado, the District of Columbia, Florida, Illinois, Louisiana, Missouri, Nevada, New Jersey, New Mexico, Pennsylvania, Virginia, Washington and Wisconsin.

VOTER REGISTRATION: THE MAJORS

Accenture Ltd.

Florida used information from Bermuda-based Accenture that led to the state's disastrous 2004 registration purge. Until 1989, it was the consulting division of former accounting firm Arthur Anderson, **Accenture** changed its name during a final split from that firm in 2001. Since then, Accenture has gained and lost statewide voter-registration system (SVRS) contracts in Colorado, Kansas and Wyoming -- in the final case, the company was forced to refund the state's money in full. Accenture is working on databases for Pennsylvania and Wisconsin. Both projects have been widely criticized, and Pennsylvania's is late. (Votingindustry.com has an **interesting overview** of Accenture's long history with e-voting technologies.)

Covansys Corp./Saber Corp.

Portland, Ore.-based **Saber** first built the Oregon registration database, then expanded to Mississippi, Montana, Maryland and Iowa. The latter states contracted with Maximus Inc. to deliver the technology for Missouri's database as well. The company acquired **Covansys**' SVRS projects when it purchased that branch of the Farmington Hills, Mich.-based company in February, though the development teams and products remain separate.

PCC Technology Group LLC

The Bloomfield, Conn.-based company that delivered the voter-registration system for Connecticut, Rhode Island and West Virginia, **PCC** has often partnered with Covansys, now part of Saber.

OTHER PLAYERS

AccuPoll Holding Corp.

This Newport Beach, Calif.-based company declared bankruptcy in January. **AccuPoll**'s e-voting technology, which lets the voter make selections on a DRE touch screen and then printed a paper ballot, has been certified for use in Texas and Missouri.

Advanced Voting Solutions Inc.

Once upon a time, Frisco, Texas-based **AVS** was known as Shoup Voting Solutions, and it built lever machines. Company founder Howard Van Pelt's previous company, Global Election Systems, grew up to be Diebold. AVS e-voting machines are or have operated in Mississippi, Pennsylvania and Virginia.

Aradyme Corp.

Orem, Utah-based **Aradyme** is subcontracted to handle data conversion on many states' voter-registration projects.

Arran Technologies Inc.
Roseville, Minn.-based **Arran**'s consultants advised Minnesota on the development of its SVRS.

Avante
Avante's Vote-Trakker 1 was the first DRE/VVPAT machine available; the latest version, Vote-Trakker 2, records votes to paper (kept behind a plastic panel, but viewable for voters to confirm before finalizing their votes) as well as to both flash memory and a hard drive. Princeton, N.J.-based Avante's machines are or have been operated in New Jersey and New York.

Automatic Voting Machine Corp.
Now defunct, Jamestown, N.Y.-based AVM built the lever machines now being phased out in New York and already retired in Louisiana and other states. It was established in 1896.

Business Records Corp. (BRC)
See **ES&S**, above.

Catalyst Computing Group Inc.
This company provides registration-database technology. Chicago-based **Catalyst** is contracted with Illinois to deliver a final version of its Help America Vote Act-compliant Illinois Voter Registration System in 2007.

Guardian Voting Systems
This is Danaher Corp.'s e-voting machines unit. States in which Gurnee, Ill.-based **Guardian Voting Systems**' machines are or have been certified are Arkansas, Delaware, Kentucky, New Mexico and Pennsylvania.

DFM Associates
As of September, Irvine, Calif.-based **DFM**'s election management software has been certified for use in California.

IVS LLC
Inspire Vote-By-Phone's e-voting technology was in wide deployment for the first time this year. Voters dial in via touch-tone phone to a computer system at a central location, monitored by election officials. The phones are situated at polling places, and a poll worker must key in his worker ID and a ballot-access ID, then hand the phone over to the voter. Louisville, Ky.-based **IVS** is certified for use in Connecticut, Maine, New Hampshire, Oklahoma, Oregon and Vermont.

MicroVote General Corp.
As of September, DRE machines from Indianapolis-based **MicroVote** were certified for use in Indiana, Kentucky and Tennessee.

Populex Corp.
This company offers e-voting technology that uses a stylus/touch-screen input to print a

bar-coded ballot card that's then scanned to record the voter's choices. As of September, Elgin, Ill.-based **Populex**'s voting technology was certified for use in Illinois and Missouri.

Quest Informations Systems Inc.
Quest sells registration-database technology. Indianapolis-based **Quest IS** developed Indiana's voter-registration database and is contracted to do the same in Virginia via an arrangement with Unisys Corp.

Saber Consulting Inc./Saber Corp.
See the registration database technology of Covansys/Saber above.

UniLect Corp.
As of September, Dublin, Calif.-based **UniLect**'s e-voting technology was certified for use in Virginia.

Vote-PAD Inc .
The Voting-on-Paper Assistive Device is a paper-based voting system geared toward use by disabled voters. As of September, **Vote-PAD**'s technology was certified in Wisconsin.

Voting Technologies International
E-voting technology. As of September, Milwaukee-based **VTI**'s DRE machines were certified in Indiana, Kansas and Wisconsin.

For more information on voter registration systems and vendors, check out **Votingindustry.com.**

See more about e-voting:

- **E-voting state by state: What you need to know**
- **Laws, lingo and technologies**
- **Review: Hacking Democracy**

Exhibit G

Anonymous Patriots. (Jul. 06, 2018). Scrap Electronic Voting Machines NOW!
Americans for Innovation.

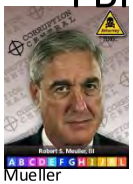
Scrap Corruption-ridden Electronic Voting – Now!

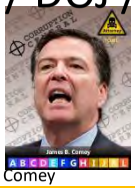
Finding: All prominent electronic voting systems in the U.S. (Smartmatic, Sequoia, Diebold, ES&S, Dominion and Hart InterCivic) are networked to the *same* software engine and controlled by the same financiers tied to George Soros and the Queen's Privy Council, thus making corrupt practices in U.S. elections a foregone conclusion. Lord Mark Malloch-Brown and Sir Geoffrey E. Pattie brag about their ability to "bend" elections , protected by the Queen.

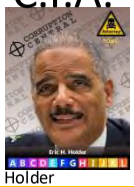
Recommendation: In addition to the companies identified below, there are other companies trying to make voting secure with jpegs, separate validations, etc. on separate machines. However, no tech of any kind can maintain a "bipartisan chain of custody." The human eye cannot see silicon circuits, software induced voltages, and that which is hidden from empirical observation. We can only 'trust' the process and the people. Electronic voting offends the entire concept of our Republic -- which was formed on the concept that authority, being given from the "power of the people" who gain it directly from God, must be separated with jurisdictional boundaries so that the "tendency of men with too much authority to 'oppress'" can be muted by that separation. Centralizing the voting process so that the 'Fake News' can report a sensationalized and profitable result is pure idiocy. We the People should not trust government. We must insist at all times and under all circumstances that dual-Federalism is maintained. The job of the People is to ensure that the boundaries are maintained. We must all be mechanics of the Republic. The following voting machines must be scrapped immediately as the fruit of a poisoned tree called technocracy.

Chief Electronic Voting Scammers:

FBI / DOJ / C.I.A.


Mueller


Comey


Holder

State Dept / DNC / RNC


Clinton


Obama


Romney


Bush

Queen's Privy Council


Soros


Malloch-Brown


Pattie

SMARTMATIC

2000 Founded in Venezuela

2004 28% Caesar Chavez-owned; offices in London UK, Caracas VZ, Boca Raton FL, Sunnyvale CA

2005 Purchased Sequoia; acquired **OpTech**

2006 Sold Sequoia-Smartmatic (US) to Smartmatic (UK)

2012 Smartmatic (UK) operated R&D labs in US, Brazil, Venezuela, Barbados, Panama, UK, Netherlands, UAE, Phillipines, Estonia and Taiwan.

2014 SGO (**Lord Malloch-Brown**) acquired Smartmatic (UK)

SEQUOIA

1960 Mathematical Systems Corp; punch cards

1970 Diamond National Corp acquired Mathematical

1983 Sequoia Pacific; acquired Diamond

1984 Sequoia Voting Machines formed from Diamond, Automatic Voting Machine Corp, **OpTech** license from Smartmatic

1997 Licensed OpTech software from Smartmatic

2005 Sequoia purchased by Smartmatic (UK)

2010 **DOJ-triggered** sale of Smartmatic to US investors (**Mitt Romney, Bain Capital**, Booz Allen), renamed company Sequoia

2011 Sold to Dominion (Canada)

2011 Filed Chapter 11 bankruptcy in US

DIEBOLD / ES&S / DOMINION

1974 Klopp Printing, Urosevich Bros, created **OpTech**; ally with Westinghouse Corp to sell Data Mark Systems

1979 Urosevich Bros and Westinghouse start American Information Systems

1997 America Info acquired ESD; renamed to Election Systems & Software (ES&S); licensed OpTech to Diebold (later renamed Premier)

1998 ES&S acquired Votronic fully electronic voting (DRE)

2006 Diebold rebranded to Premier Election Systems

2009 ES&S acquired Premier

2010 Dominion Voting Systems acquired Premier (formerly Diebold) in a **DOJ-triggered** anti-trust divestiture

HART INTERCIVIC

2000 Hart InterCivic spun off from Hart Graphics to focus on election systems

2010 **Mitt Romney, Bain Capital**, Booz Allen purchased Smartmatic (US); acquires **OpTech** license from **DOJ-triggered** sale; renamed it Sequoia

LORD MALLOCH-BROWN

2010 Avid introduced **LeaderPlus** Election Night Newsroom management suite

2012 Investec Plc , Malloch-Brown invested in **ISIS Management Limited** (**Investec Plc**); Avid introduced **Avid Knowledge Base ISIS Management Console** - Agent Settings as complement to LeaderPlus; pushes Fake News scripts to MSM election news anchors in real time

Exhibit H

Phillip A. Brooks, (Sep. 18, 2015). Re. Notice of Violation, Volkswagen Software Hack To Modify Test Conditions Automatically. United States Environmental Protection Agency.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

SEP 18 2015

OFFICE OF
ENFORCEMENT AND
COMPLIANCE ASSURANCE

VIA CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Volkswagen AG
Audi AG
Volkswagen Group of America, Inc.
Thru:

David Geanacopoulos
Executive Vice President Public Affairs and General Counsel
Volkswagen Group of America, Inc.
2200 Ferdinand Porsche Drive
Herndon, VA 20171

Stuart Johnson
General Manager
Engineering and Environmental Office
Volkswagen Group of America, Inc.
3800 Hamlin Road
Auburn Hills, MI 48326

Re: Notice of Violation

Dear Mr. Geanacopoulos and Mr. Johnson:

The United States Environmental Protection Agency (EPA) has investigated and continues to investigate Volkswagen AG, Audi AG, and Volkswagen Group of America (collectively, VW) for compliance with the Clean Air Act (CAA), 42 U.S.C. §§ 7401–7671q, and its implementing regulations. As detailed in this Notice of Violation (NOV), the EPA has determined that VW manufactured and installed defeat devices in certain model year 2009 through 2015 diesel light-duty vehicles equipped with 2.0 liter engines. These defeat devices bypass, defeat, or render inoperative elements of the vehicles' emission control system that exist to comply with CAA emission standards. Therefore, VW violated section 203(a)(3)(B) of the CAA, 42 U.S.C. § 7522(a)(3)(B). Additionally, the EPA has determined that, due to the existence of the defeat

devices in these vehicles, these vehicles do not conform in all material respects to the vehicle specifications described in the applications for the certificates of conformity that purportedly cover them. Therefore, VW also violated section 203(a)(1) of the CAA, 42 U.S.C. § 7522(a)(1), by selling, offering for sale, introducing into commerce, delivering for introduction into commerce, or importing these vehicles, or for causing any of the foregoing acts.

Law Governing Alleged Violations

This NOV arises under Part A of Title II of the CAA, 42 U.S.C. §§ 7521–7554, and the regulations promulgated thereunder. In creating the CAA, Congress found, in part, that "the increasing use of motor vehicles . . . has resulted in mounting dangers to the public health and welfare." CAA § 101(a)(2), 42 U.S.C. § 7401(a)(2). Congress' purpose in creating the CAA, in part, was "to protect and enhance the quality of the Nation's air resources so as to promote the public health and welfare and the productive capacity of its population," and "to initiate and accelerate a national research and development program to achieve the prevention and control of air pollution." CAA § 101(b)(1)–(2), 42 U.S.C. § 7401(b)(1)–(2). The CAA and the regulations promulgated thereunder aim to protect human health and the environment by reducing emissions of nitrogen oxides (NOx) and other pollutants from mobile sources of air pollution. Nitrogen oxides are a family of highly reactive gases that play a major role in the atmospheric reactions with volatile organic compounds (VOCs) that produce ozone (smog) on hot summer days. Breathing ozone can trigger a variety of health problems including chest pain, coughing, throat irritation, and congestion. Breathing ozone can also worsen bronchitis, emphysema, and asthma. Children are at greatest risk of experiencing negative health impacts from exposure to ozone.

The EPA's allegations here concern light-duty motor vehicles for which 40 C.F.R. Part 86 sets emission standards and test procedures and section 203 of the CAA, 42 U.S.C. § 7522, sets compliance provisions. Light-duty vehicles must satisfy emission standards for certain air pollutants, including NOx. 40 C.F.R. § 86.1811-04. The EPA administers a certification program to ensure that every vehicle introduced into United States commerce satisfies applicable emission standards. Under this program, the EPA issues certificates of conformity (COCs), and thereby approves the introduction of vehicles into United States commerce.

To obtain a COC, a light-duty vehicle manufacturer must submit a COC application to the EPA for each test group of vehicles that it intends to enter into United States commerce. 40 C.F.R. § 86.1843-01. The COC application must include, among other things, a list of all auxiliary emission control devices (AECDs) installed on the vehicles. 40 C.F.R. § 86.1844-01(d)(11). An AECD is "any element of design which senses temperature, vehicle speed, engine RPM, transmission gear, manifold vacuum, or any other parameter for the purpose of activating, modulating, delaying, or deactivating the operation of any part of the emission control system." 40 C.F.R. § 86.1803-01. The COC application must also include "a justification for each AECD, the parameters they sense and control, a detailed justification of each AECD that results in a reduction in effectiveness of the emission control system, and [a] rationale for why it is not a defeat device." 40 C.F.R. § 86.1844-01(d)(11).

A defeat device is an AECD "that reduces the effectiveness of the emission control system under conditions which may reasonably be expected to be encountered in normal vehicle operation and

use, unless: (1) Such conditions are substantially included in the Federal emission test procedure; (2) The need for the AECD is justified in terms of protecting the vehicle against damage or accident; (3) The AECD does not go beyond the requirements of engine starting; or (4) The AECD applies only for emergency vehicles . . . ." 40 C.F.R. § 86.1803-01.

Motor vehicles equipped with defeat devices, such as those at issue here, cannot be certified. EPA, *Advisory Circular Number 24: Prohibition on use of Emission Control Defeat Device* (Dec. 11, 1972); *see also* 40 C.F.R. §§ 86-1809-01, 86-1809-10, 86-1809-12. Electronic control systems which may receive inputs from multiple sensors and control multiple actuators that affect the emission control system's performance are AECDs. EPA, *Advisory Circular Number 24-2: Prohibition of Emission Control Defeat Devices – Optional Objective Criteria* (Dec. 6, 1978). "Such elements of design could be control system logic (i.e., computer software), and/or calibrations, and/or hardware items." *Id.*

"Vehicles are covered by a certificate of conformity only if they are in all material respects as described in the manufacturer's application for certification . . . ." 40 C.F.R. § 86.1848-10(c)(6). Similarly, a COC issued by EPA, including those issued to VW, state expressly, "[t]his certificate covers only those new motor vehicles or vehicle engines which conform, in all material respects, to the design specifications" described in the application for that COC. *See also* 40 C.F.R. §§ 86.1844-01 (listing required content for COC applications), 86.1848-01(b) (authorizing the EPA to issue COCs on any terms that are necessary or appropriate to assure that new motor vehicles satisfy the requirements of the CAA and its regulations).

The CAA makes it a violation "for any person to manufacture or sell, or offer to sell, or install, any part or component intended for use with, or as part of, any motor vehicle or motor vehicle engine, where a principal effect of the part or component is to bypass, defeat, or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter, and where the person knows or should know that such part or component is being offered for sale or installed for such use or put to such use." CAA § 203(a)(3)(B), 42 U.S.C. § 7522(a)(3)(B); 40 C.F.R. § 86.1854-12(a)(3)(ii). Additionally, manufacturers are prohibited from selling, offering for sale, introducing into commerce, delivering for introduction into commerce, or importing, any new motor vehicle unless that vehicle is covered by an EPA-issued COC. CAA § 203(a)(1), 42 U.S.C. § 7522(a)(1); 40 C.F.R. § 86.1854-12(a)(1). It is also a violation to cause any of the foregoing acts. CAA § 203(a), 42 U.S.C. § 7522(a); 40 C.F.R. § 86-1854-12(a).

Alleged Violations

Each VW vehicle identified by the table below has AECDs that were not described in the application for the COC that purportedly covers the vehicle. Specifically, VW manufactured and installed software in the electronic control module (ECM) of these vehicles that sensed when the vehicle was being tested for compliance with EPA emission standards. For ease of reference, the EPA is calling this the "switch." The "switch" senses whether the vehicle is being tested or not based on various inputs including the position of the steering wheel, vehicle speed, the duration of the engine's operation, and barometric pressure. These inputs precisely track the parameters of the federal test procedure used for emission testing for EPA certification purposes. During EPA

emission testing, the vehicles' ECM ran software which produced compliant emission results under an ECM calibration that VW referred to as the "dyno calibration" (referring to the equipment used in emissions testing, called a dynamometer). At all other times during normal vehicle operation, the "switch" was activated and the vehicle ECM software ran a separate "road calibration" which reduced the effectiveness of the emission control system (specifically the selective catalytic reduction or the lean NOx trap). As a result, emissions of NOx increased by a factor of 10 to 40 times above the EPA compliant levels, depending on the type of drive cycle (e.g., city, highway).

The California Air Resources Board (CARB) and the EPA were alerted to emissions problems with these vehicles in May 2014 when the West Virginia University's (WVU) Center for Alternative Fuels, Engines & Emissions published results of a study commissioned by the International Council on Clean Transportation that found significantly higher in-use emissions from two light duty diesel vehicles (a 2012 Jetta and a 2013 Passat). Over the course of the year following the publication of the WVU study, VW continued to assert to CARB and the EPA that the increased emissions from these vehicles could be attributed to various technical issues and unexpected in-use conditions. VW issued a voluntary recall in December 2014 to address the issue. CARB, in coordination with the EPA, conducted follow up testing of these vehicles both in the laboratory and during normal road operation to confirm the efficacy of the recall. When the testing showed only a limited benefit to the recall, CARB broadened the testing to pinpoint the exact technical nature of the vehicles' poor performance, and to investigate why the vehicles' onboard diagnostic system was not detecting the increased emissions. None of the potential technical issues suggested by VW explained the higher test results consistently confirmed during CARB's testing. It became clear that CARB and the EPA would not approve certificates of conformity for VW's 2016 model year diesel vehicles until VW could adequately explain the anomalous emissions and ensure the agencies that the 2016 model year vehicles would not have similar issues. Only then did VW admit it had designed and installed a defeat device in these vehicles in the form of a sophisticated software algorithm that detected when a vehicle was undergoing emissions testing.

VW knew or should have known that its "road calibration" and "switch" together bypass, defeat, or render inoperative elements of the vehicle design related to compliance with the CAA emission standards. This is apparent given the design of these defeat devices. As described above, the software was designed to track the parameters of the federal test procedure and cause emission control systems to underperform when the software determined that the vehicle was not undergoing the federal test procedure.

VW's "road calibration" and "switch" are AECDs[1] that were neither described nor justified in the applicable COC applications, and are illegal defeat devices. Therefore each vehicle identified by the table below does not conform in a material respect to the vehicle specifications described in the COC application. As such, VW violated section 203(a)(1) of the CAA, 42 U.S.C. § 7522(a)(1), each time it sold, offered for sale, introduced into commerce, delivered for introduction into commerce, or imported (or caused any of the foregoing with respect to) one of the hundreds of thousands of new motor vehicles within these test groups. Additionally, VW

[1] There may be numerous engine maps associated with VW's "road calibration" that are AECDs, and that may also be defeat devices. For ease of description, the EPA is referring to these maps collectively as the "road calibration."

violated section 203(a)(3)(B) of the CAA, 42 U.S.C. § 7522(a)(3)(B), each time it manufactured and installed into these vehicles an ECM equipped with the "switch" and "road calibration."

The vehicles are identified by the table below. All vehicles are equipped with 2.0 liter diesel engines.

Model Year	EPA Test Group	Make and Model(s)
2009	9VWXV02.035N	VW Jetta, VW Jetta Sportwagen
2009	9VWXV02.0U5N	VW Jetta, VW Jetta Sportwagen
2010	AVWXV02.0U5N	VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2011	BVWXV02.0U5N	VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2012	CVWXV02.0U5N	VW Beetle, VW Beetle Convertible, VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2012	CVWXV02.0U4S	VW Passat
2013	DVWXV02.0U5N	VW Beetle, VW Beetle Convertible, VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2013	DVWXV02.0U4S	VW Passat
2014	EVWXV02.0U5N	VW Beetle, VW Beetle Convertible, VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2014	EVWXV02.0U4S	VW Passat
2015	FVGAV02.0VAL	VW Beetle, VW Beetle Convertible, VW Golf, VW Golf Sportwagen, VW Jetta, VW Passat, Audi A3

Enforcement

The EPA's investigation into this matter is continuing. The above table represents specific violations that the EPA believes, at this point, are sufficiently supported by evidence to warrant the allegations in this NOV. The EPA may find additional violations as the investigation continues.

The EPA is authorized to refer this matter to the United States Department of Justice for initiation of appropriate enforcement action. Among other things, persons who violate section 203(a)(3)(B) of the CAA, 42 U.S.C. § 7522(a)(3)(B), are subject to a civil penalty of up to $3,750 for each violation that occurred on or after January 13, 2009;[1] CAA § 205(a), 42 U.S.C. § 7524(a); 40 C.F.R. § 19.4. In addition, any manufacturer who, on or after January 13, 2009, sold, offered for sale, introduced into commerce, delivered for introduction into commerce, imported, or caused any of the foregoing acts with respect to any new motor vehicle that was not covered by an EPA-issued COC is subject, among other things, to a civil penalty of up to $37,500 for each violation.[2] CAA § 205(a), 42 U.S.C. § 7524(a); 40 C.F.R. § 19.4. The EPA may seek, and district courts may order, equitable remedies to further address these alleged violations. CAA § 204(a), 42 U.S.C. § 7523(a).

[1] $2,750 for violations occurring prior to January 13, 2009.
[2] $32,500 for violations occurring prior to January 13, 2009.

The EPA is available to discuss this matter with you. Please contact Meetu Kaul, the EPA attorney assigned to this matter, to discuss this NOV. Ms. Kaul can be reached as follows:

Meetu Kaul
U.S. EPA, Air Enforcement Division
1200 Pennsylvania Avenue, NW
William Jefferson Clinton Federal Building
Washington, DC 20460
(202) 564-5472
kaul.meetu@epa.gov

Sincerely,

Phillip A. Brooks
Director
Air Enforcement Division
Office of Civil Enforcement

Copy:
Todd Sax, California Air Resources Board
Walter Benjamin Fisherow, United States Department of Justice
Stuart Drake, Kirkland & Ellis LLP

July 11, 2018

Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers

Testifying at Senate Rules Committee, Wyden Blasts Voting Machine Manufacturers, Calls for Passage of His Bill Mandating Paper Ballots

Washington, D.C. – Sen. Ron Wyden, D-Ore., sounded the alarm about the urgent need for paper ballots to secure American elections against foreign hackers, in testimony at the Senate Rules Committee today.

Wyden called on the Senate to pass his Protecting American Votes and Elections Act, which requires paper ballots and effective audits for all federal elections, and has been endorsed by leading cybersecurity experts. View his full testimony here.

"At least 44 million Americans - and perhaps millions more - have no choice but to use insecure voting machines that have foreign hackers salivating," Wyden said. **"It is inexcusable that American democracy depends on hackable voting technology made by a handful of companies that have evaded oversight and stonewalled Congress. That must end."**

Wyden blasted voting machine companies for refusing to answer basic questions about their cybersecurity practices. ES&S continued to stonewall Wyden's questions even after the New York Times reported the company had sold voting technology with remote monitoring software installed.

"The only way to make this worse would be to leave unguarded ballot boxes in Moscow and Beijing," Wyden said. **"Americans must move to paper ballots, marked by hand. Until that system is adopted, every election that goes by is an election that Russia could hack."**

###

Exhibit J

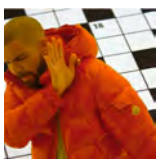
Kim Zetter. (Jul. 17, 2018). Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States. *Motherboard*.

PCANYWHERE

Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States

Remote-access software and modems on election equipment 'is the worst decision for security short of leaving ballot boxes on a Moscow street corner.'

By Kim Zetter | Jul 17 2018, 5:00am



UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

The nation's top voting machine maker has admitted in a letter to a federal lawmaker that the company installed remote-access software on election-management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them.

In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had "provided pcAnywhere remote connection software ... to a small number of customers between 2000 and 2006," which was installed on the election-management system ES&S sold them.

The statement contradicts what the company **told me and fact checkers for a story I wrote for the *New York Times*** in February. At that time, a spokesperson said ES&S had never installed pcAnywhere on any election system it sold. "None of the employees, ... including long-tenured employees, has any knowledge that our voting systems have ever been sold with remote-access software," the spokesperson said.

ES&S did not respond on Monday to questions from Motherboard, and it's not clear why the company changed its response between February and April. Lawmakers, however, have subpoena powers that can compel a company to hand over documents or provide sworn testimony on a matter lawmakers are investigating, and a statement made to lawmakers

Trump's Stupid 'Where Is the DNC Server?' Conspiracy Theory, Explained

Trump refuses to believe all the evidence that Russia hacked the DNC, because he understands nothing about how digital forensics works.

Motherboard / Jason Koebler / Jul 16

ES&S is the top voting machine maker in the country, a position it held in the years 2000-2006 when it was installing pcAnywhere on its systems. The company's machines were used statewide in a number of states, and

The company told Wyden it stopped installing pcAnywhere on systems in December 2007, after the Election Assistance Commission, which oversees the federal testing and certification of election systems used in the US, released new voting system standards. Those standards required that any election system submitted for federal testing and certification thereafter could contain only software essential for voting and tabulation. Although the standards only went into effect in 2007, they were created in 2005 in a very public process during which the security of voting machines was being discussed frequently in newspapers and on Capitol Hill.

Election-management systems are not the voting terminals that voters use to cast their ballots, but are just as critical: they sit in county election offices and contain software that in some counties is used to program all

upgrade or alter software. But election-management systems and voting machines are supposed to be air-gapped for security reasons—that is, disconnected from the internet and from any other systems that are connected to the internet. ES&S customers who had pcAnywhere installed also had modems on their election-management systems so ES&S technicians could dial into the systems and use the software to troubleshoot, thereby creating a potential port of entry for hackers as well.

In May 2006 in Allegheny County, Pennsylvania, ES&S technicians used the pcAnywhere software installed on that county's election-management system for hours trying to reconcile vote discrepancies in a local election, according to **a report** filed at the time. And in a **contract with Michigan**, which covered 2006 to 2009, ES&S discussed its use of pcAnywhere and modems for this purpose.

"In some cases, the Technical Support representative accesses the customer's system through PCAnywhere—off-the-shelf software which allows immediate access to the customer's data and network system from a remote location—to gain insight into the issue and offer precise solutions," ES&S wrote in a June 2007 addendum to the contract. "ES&S technicians can use PCAnywhere to view a client computer, assess the exact situation that caused a software issue and to view data files."

Motherboard asked a Michigan spokesman if any officials in his state ever

security vulnerabilities. If an attacker can gain remote access to an election-management system through the modem and take control of it using the pcAnywhere software installed on it, he can introduce malicious code that gets passed to voting machines to disrupt an election or alter results.

Wyden told Motherboard that installing remote-access software and modems on election equipment "is the worst decision for security short of leaving ballot boxes on a Moscow street corner."

In 2006, the same period when ES&S says it was still installing pcAnywhere on election systems, hackers **stole the source code for the pcAnyhere software**, though the public didn't learn of this until years later in 2012 when a hacker posted some of the source code online, forcing Symantec, the distributor of pcAnywhere, to admit that it had been stolen years earlier. Source code is invaluable to hackers because it allows them to examine the code to find security flaws they can exploit. When Symantec admitted to the theft in 2012, it took the unprecedented step of **warning users to disable or uninstall the software** until it could make sure that any security flaws in the software had been patched.

UP NEXT

Solve the Internet Crossword Puzzle: August 1, 2018

Around this same time, security researchers **discovered a critical vulnerability** in pcAnywhere that would allow an attacker to seize control of a system that had the software installed on it, without needing to authenticate themselves to the system with a password. And other researchers with the security firm Rapid7 scanned the internet for any computers that were online and had pcAnywhere installed on them and found nearly 150,000 were configured in a way that would allow direct access to them.

It's not clear if election officials who had pcAnywhere installed on their systems, ever patched this and other security flaws that were in the software.

"[I]t's very unlikely that jurisdictions that had to use this software ... updated it very often," says Joseph Lorenzo Hall, chief technologist for the Center for Democracy and Technology, "meaning it's likely that a non-

only to dial out, not receive calls, so that only election officials could initiate connections with ES&S. But when Wyden's office asked in a letter to ES&S in March what settings were used to secure the communications, whether the system used hard-coded or default passwords and whether ES&S or anyone else had conducted a security audit around the use of pcAnywhere to ensure that the communication was done in a secure manner, the company did not provide responses to any of these questions.

Even if ES&S and its customers configured their remote connections to ES&S in a secure manner, the recent **US indictments against Russian state hackers** who tried to interfere in the 2016 presidential elections, show that they targeted companies in the US that make software for the administration of elections. An attacker would only have had to hack ES&S and then use its network to slip into a county's election-management system when the two systems made a remote connection.

In its letter to Wyden, ES&S defended its installation of pcAnywhere, saying that during the time it installed the software on customer machines prior to 2006, this was "considered an accepted practice by numerous technology companies, including other voting system manufacturers."

Motherboard contacted two of the top vendors—Hart InterCivic and Dominion—to verify this, but neither responded. However, Douglas Jones,

their contracts with customers included the requirement of a remote-login port allowing [the company] to have remote access to the customer system in order to allow customer support."

He notes that election officials who purchased the systems likely were not aware of the potential risks they were taking in allowing this and didn't understand the threat landscape to make intelligent decisions about installing such software.

All of this raises questions about how many counties across the US had remote-access software installed—in addition to ES&S customers—and whether intruders had ever leveraged it to subvert elections.

Although Wyden's office asked ES&S to identify which of its customers were sold systems with pcAnywhere installed, the company did not respond. ES&S would only say that it had confirmed with customers who had the software installed that they "no longer have this application installed."

The company didn't respond to questions from Motherboard asking when these customers removed the software—whether ES&S had instructed them to do so back in 2007 when the company says it stopped installing the software on new systems it sold or whether it had only recently told customers to remove it following concerns raised in the 2016 presidential elections that Russian hackers were targeting election networks in the US.

Exhibit K

OKANOGAN County Election Procedures

These documents are too voluminous, and will therefore be made available upon request pursuant to Wash. R. Evid. 1006 and related rules.

1. Public Records available upon request from Okanogan County Auditor
2. Basic Instructions
    a. 10-03 Clearinghouse Judicial Elections and Exceptions 2010.pdf
    b. Election Emergency Procedures.doc
    c. Good Vote Bad Vote Poster 2.pdf
    d. Instructions - Preparing Notice of Election.docx
    e. Observer's Guide.pdf
    f. Seal Logs.doc
3. Misc. Instructions
    a. After Election
        i. Mail merge for after certification.doc
        ii. BN Instructions scan and resolve.doc
        iii. Test Election Database.docx
    b. Ballot now
        i. BN Instructions scan and resolve.doc
        ii. Test Election Database.docx
4. Ballots
    a. 1 Extract, Upload ballot, print labels, and voter list - updated.docx
    b. Checking ballots back from the printer. docMail
    c. Certification to OSOS.docx
    d. Placement of issue and offices on ballot.doc
    e. Preparing to print envelopes.doc
5. Canvass Board

a. Ballot to Canvass Board log.doc
    b. Ballots to Canvass Board Master.doc

    c. Canvass.docx
    d. Certify.docx
6. Inspection Boards
    a. WAC 434 Ballot inspection.doc
7. Voter Registration
    a. List of Voters for each election.doc
8. Voting equipment – HART
    a. Processing of ballots as defined in WAC 434.doc
9. WEI
    a. Set candidate statement word length WEI.docx
    b. Testing MyBallot.doc
    c. Turn on MyBallot Ballot Status for UOCAVA Ballots.doc
    d. WEI Candidate filing.pdf
    e. WEI election results Ballots left to count.docx
10. Procedure manual
    a. 10 Elections Department Policy Placement on ballot.pdf
    b. 10-03 Clearinghouse Judicial Elections and Exceptions 2010.pdf
    c. Canvass Board Manual.pdf
    d. Instructions for BOSS Setup.docx
    e. New Procedures Canvass Board 2017.doc
    f. Placement of issue and offices on ballot.doc
    g. Procedures 1 - Voter Registration.doc
    h. Procedures 2 - Election Envelopes, Inactive, Special ballots.doc
    i. Procedures Canvass Board 2017.doc
    j. Procedures Canvass Board 2017.pdf
11. Votec Instructions
    a. Ballot Log.doc
    b. Ballots returned undeliverable.doc
    c. Ballots that need proof of ID.doc
    d. Ballots that were forwarded and you got a notice from the Post Office.doc
    e. Candidate Filing.doc
    f. Candidate Module 1.doc
    g. Candidate Module.doc
    h. Change Notice Letters.doc
    i. Change status of voter from Inactive to Active.doc
    j. Checking signatures.doc
    k. Create an absentee list to be emailed.doc
    l. Election night issue ballots.doc
    m. Election Setup.doc
    n. Get totals of ballots sent and ballots returned.doc
    o. Getting totals of ballots in and out for an election.doc
    p. Handle duplicate registrations.doc
    q. How to get a list of voters with DLV.doc
    r. Inactive Purge.doc
    s. Issuing a ballot over the counter.doc
    t. List of return ballots.doc

u. Lists of ballots in.doc
v. Move winning candidates forward from Primary to General - Copy.doc
w. New registrations after the initial loading of ballots that are in By Mail Precincts or Request Ongoing Ballots.doc
x. Non ID compliant purge.docx
y. Odd year preparation.docx
z. Preparing for an election with State VRDB.doc
aa. Print Mailing Label Dymo for envelope Non ballot.doc
bb. Printing a Precinct with District List.doc
cc. Printing the report of previous registrations.doc
dd. Procedure changes.doc
ee. Process Exceptions.docx
ff. Provisional Ballots.doc
gg. Public Instruction for ballots that were forwarded, and you got a notice from the Post
hh. Offic1.doc
ii. Registration Totals for an election.docx
jj. Remove cancelled voters from election.doc
kk. Report number of ballots requested and received.doc
ll. Update or change Elected Officials list.doc
mm. Update voters who voted a Provisional Ballot.doc
nn. Upload ballot print labels, and voter list.docx
oo. Use of Disabled Access units.doc
pp. VOTEC Candidate File.docx
qq. Voter Stats.docx
rr. When an incorrect serial number was entered, and the wrong person was updated.docx
ss. Using DAU unit.doc

12. 2008 Instructions
    a. New resolve instructions 2008.doc
    b. New Scan instructions 2008.doc
13. Ballot Now
    a. 2012 Ballot Scanning - Resolution - Boards .doc
    b. BACK UP VOTING SYSTEM.doc
    c. Ballot Now Sequential Steps to start up.doc
    d. Print ballot images for the Printer.doc
    e. Write-Ins.doc
14. Instructions for Tally
    a. Finalize Tally after Election Certification.doc
    b. Set up new election database.doc

Exhibit L

James M. Miller. (August 5, 2018). Professional Experience and Resume.

James M. Miller

Professional Experience & Resume

Updated August 5, 2018

Project Management, Business Process, Quality Control and Data Science

I, James M. Miller, worked at Boeing for 17 years in various positions and assignments, mostly as a Project Manager while earning two master's Certificates in Project Management (academic and technical).

For seven of these years, the Petitioner was assigned to Cabin Systems Material as a subject matter expert for new technology for the Boeing interiors, including new In-flight entertainment, satellite communications, and the Boeing contract manager for Connection by Boeing. Ref: (https://en.wikipedia.org/wiki/Connexion_by_Boeing).

During this time period, I was assigned the task of developing a new Boeing business process which resulted in the new Boeing business process BPI-4232, know as "Customer Selected Equipment (CSE)." This resolved the manufacturing conflicts when new technology was desired by the customer demanding that Boeing install the new systems on the customer airlines.

Previous to CSE, supplemental type certifications (STE), were used to qualify new systems as retrofit on existing aircraft. This caused complex manufacturing issues and waste in the Boeing build line, causing delays estimated to be over $400 million per year. I led a team of engineers, finance, supply managers, and customer engineers, CSE was created where pre-qualification data for new technology was first reviewed by Boeing engineering as a fee based contract. I negotiated and managed over $50 million of these initial contracts while in this position.

The CSE process required three years of process review that included manufacturing engineering, multiple vendor engineering, quality reviews, industrial design processes for new equipment, and thousands of hours of overall process design meetings around the globe. The CSE process enabled a multi-billion dollar industry to flourish around the globe. A similar process was adopted by Airbus.

The Petitioner also worked seven years within Boeing's Cabin System Engineering group, assigned as a project manager for the development of over $34 million dollars in new technology for avionics, cabin server, terminal wireless LAN, video surveillance, and other projects. A notable project of relevance was the Emirates Airline First Class Seat Failure. I was

assigned to manage the investigation and solution of Emirate's very expensive seat failures, given unlimited authority and resources of the Boeing company, to rapidly resolve the issue. I gathered a team of scientists and engineers from Phantom Works, Crane Electronics, Boeing Electronics, and Panasonic Corporation.

Upon examination under electron microscopy of the suspected integrated circuits involved in the seat and supporting Boeing systems, hidden circuits operated by bootlegged undetectable machine language, was discovered in related vendor circuit. This circuit had not been discovered during 'red label' testing, nor properly disclosed by the vendor. This resulted in the decertification, heavy fines, and very bad press with the vendor's airline customers, and a major recall/replacement plan of all of the vendor's part numbers.

The notable part of this testimony is that hidden integrated circuits and bootlegged machine language is possible even under highly scrutinized aerospace procedures. I also worked on other avionics boxes that had to interface with the main airplane computer, or MCU; requiring failure modes analysis of degrees of ten to the ninth (10^9) in order to pass FAA flight regulations. The process control, review, understanding, and acceptance of software, hardware, and signal interfaces is tedious to develop, but necessary for flight safety. Because of this, airplanes do not fall out of the sky with any regularity, or due to systems failure. Almost all airplane failure is operational or administrative involving bad decisions.

I also worked 25 years in the municipal utility industry, obtaining many training certificates involving safety processes, hydraulic and chemical engineering, computer programming in multiple languages, Supervisory Control and Data Acquisition (SCADA) for automating pumping systems, alarms, and basic data telemetry. This often involved a forensic analysis of acquired data with database programming to make and test failure hypotheses to correct intrinsic failure modes. I was certified at the highest operational level with the State of Washington as a WDM-IV.

Currently, I am the Chief Operating Officer (CEO), of Core Data Analytics, where I oversee the daily operations and development of business operations software for government and private business. www.easyops.co I also serve as the business analyst and database designer, ensuring that the database design is efficiently developed to the 5th Normal form—a mathematical formula to produce the least amount of data necessary to reassemble datum into information. https://en.wikipedia.org/wiki/Boyce%E2%80%93Codd_normal_form.

I have extensive experience and education as an expert in project management, forensic processes, troubleshooting, quality control, design and control of complex systems.

System Security

Voters can rest assured that Washington's Election system is secure.

We have embarked on an unprecedented opportunity to work collaboratively with the Department of Homeland Security to ensure that our election systems remain secure. This partnership allows us to work together, elections and IT experts working hand in hand to ensure our systems are secure.

We are thrilled to partner with DHS to –

- Assess vulnerabilities and identify mitigation plans
- Share information
- Rely on DHS for local in person support
- Report incidents or threats

Some highlights of the programs already underway –

The Risk and Vulnerability Assessment (RVA) - The RVA encompasses a wide range of security services including –

- Penetration testing
- Web application testing
- Social engineering

Cyber Resilience Review (CRR) - The CRR measures and enhances the implementation of key cybersecurity capacities and capabilities of critical infrastructure and SLTT governmental entities. This is a non-technical assessment helps the assessed organization to develop an understanding of their operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress or crisis.

This DHS partnership provides all of these services to us at no cost.

In addition, Washington employs the recommendations raised by security experts, and have done so for years. Such as –

- Paper-based systems, including voter verifiable paper audit trails.
- Independent testing.
- Pre- and post-election audits.
- Physical security of tabulation equipment.

Before a tabulation system can be used in Washington, we require testing at a federally approved independent testing lab. These expert testers include security reviews as a part of their overall testing efforts. Then, systems are tested here at the state level and reviewed by

our own voting systems certification board, comprised of technology experts, accessibility experts, and county election officials.

Counties must then perform acceptance testing and logic and accuracy testing prior to every election. In addition, we conduct post-election audits, where we draw precincts and races at random and compare the vote totals from the tabulator to a hand count of ballots before the election is certified.

Counties that *optically* scan ballots prior to Election Day have approved tabulation security plans in place and on file with our office. Additionally, counties maintain continuity of operations plans so that they can be ready in the event of a disruption. We are present at logic and accuracy tests where we review and ensure, both visually and through hash testing, that the equipment and software in use hasn't changed from the version certified both federally and in Washington.

We use a paper-based system, which always allows Washington elections officials the opportunity to see first-hand the voter's intent. We can go back to the paper ballot marked by the voter and hand count a race, particularly when the races are very close. And for the few voters who are voting on touch screen voting systems, we require a paper audit trail verified by the voter.

In addition, we work proactively and closely with IT and security experts to routinely review, identify, and correct any vulnerabilities with our technical systems.

Washington has a long-standing tradition of balancing this physical security with technical system security and providing accessible systems to our voters.

In addition to the security of our tabulation systems, Washington takes great pride in securing our other vital systems. The Voter registration Database (VRDB) and Washington Elections Information (WEI) systems are secured by highly skilled Office of the Secretary of State (OSOS) IT staff, using state of the art equipment and following IT industry best practices.

Network Based Security:

- All elections systems are protected by state of the art Intrusion Prevention Systems (IPS) and firewalls. Only authorized Internet Protocol (IP) address are allowed access to these systems. This access is running on a network that is only used by authorized partners and the accessible web servers are isolated on a network demilitarized zone (DMZ) with the database servers placed in another secured inside a isolated network.

Physical Security:

- The servers are housed in a secure single tenant modern facility with dual redundant alarms, security cameras, and FM200 protection. Physical access to the data center is restricted to only three authorized OSOS full-time IT staff members using security proximity cards and unique keypad pin numbers. The data center is located next door to the police station and response times for alarms average 2 to 8 minutes.

Patch Management:

- The Quality Assurance (QA) system is patched the day after any “patches”, “hotfixes”, or “cumulative” updates are received from Microsoft. Production (prod) servers are patched after the system updates are fully tested in QA and authorized for deployment. In most cases, the production system patched two weeks after QA to allow for testing and verification.

Security Audit:

- Regular security scans by OSOS IT security staff are performed to test and verify the security of the firewalls, IPS, and servers.
- Periodic 3rd party contracted security audits are performed to test and verify the security and effectiveness of the firewalls, IPS, servers, and facility.

Log Review:

- Daily firewall logs are reviewed at least 4 times a day and weekend logs are reviewed every Monday morning.
- Daily system event logs are reviewed at least twice a day and weekend logs are reviewed every Monday morning.

Elections Results Site

- The elections results are hosted in Microsoft’s Azure cloud, which provides server and geographic redundancy.
- Results data is retrieved from a secure location provided by Washington Election Information System (WEI) at specified times (intervals).
- Elections results data is parsed and presented to users graphically in read-only and compact web files (html) for speed and performance under heavy user access.
- Graphic representation of the results is not connected to WEI system or network and is not dependent on it after results have been securely transmitted at aforementioned intervals.

Tabulation Systems

Before a system can be considered for state certification, it must be first tested by an independent testing authority that has been accredited by the Election Assistance Commission. There currently are three test labs (certified independent testing authorities) that are accredited by the Election Assistance Commission. NTS Huntsville, Pro V&V, and SLI Compliance. You can find more information about those accreditations here: https://www.eac.gov/testing_and_certification/accredited_test_laboratories.aspx (https://www.eac.gov/testing_and_certification/accredited_test_laboratories.aspx)

All voting system testing documentation, which includes the test lab identification, can be found here: https://www.eac.gov/testing_and_certification/default.aspx (https://www.eac.gov/testing_and_certification/default.aspx). When reviewing these testing

documents, keep in mind that not all of these systems are certified for use in the State of Washington. The list of systems certified for using the State of Washington can be found here: https://www.sos.wa.gov/elections/research/Voting-System-Testing-and-Certification.aspx (https://www.sos.wa.gov/elections/research/Voting-System-Testing-and-Certification.aspx). A list of voting systems that are in use by county can be found here: https://www.sos.wa.gov/elections/research/Voting-Systems-by-County.aspx (https://www.sos.wa.gov/elections/research/Voting-Systems-by-County.aspx)

No tabulation equipment is connected to the internet or capable of wireless communication. Additionally, WAC 434-261-045 requires that security measures be employed to detect any inappropriate access to protect the physical security of the system. That could include video surveillance, however, that is not required. Counties can employ multiple layers of physical security that would detect inappropriate access, for example, logs and seals.

FORTUNE

This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings

By **DON REISINGER** October 17, 2017

A site that ranks companies based on their commitment to conservative values has some problems with some of Silicon Valley's biggest names.

On Tuesday, Bloomberg published an interview with David Black, the co-founder and former CEO of Aegis Science, and the husband to Republican representative Diane Black, herself a co-founder in Aegis. In that interview, Black described a site that he's built with more than $1 million of his money called 2ndVote. The goal: to determine how closely companies hold conservative values and rank them on a scale of one to five, with one being most liberal and five as most conservative.

In its look at rankings, 2ndVote appears to have given some of the most major tech companies generally have low scores.

Amazon

Amazon (AMZN, +0.33%) generated a score of 1.9 out of five in the 2ndVote test.

According to 2ndVote, the e-commerce giant scored low marks for prohibiting the sale of firearms on its site and its support for the "liberal 2015 Paris climate deal" as a problem.

However, Amazon got some points back for supporting the Salvation Army, which 2ndVote describes as "a group supporting traditional marriage" and "a pro-life organization."

Apple

Apple (AAPL, -0.32%) came in at the bottom of the 2ndVote scale with a rating of one out of five.

In every metric 2ndVote considers, including gun rights, the environment, marriage, life, and immigration, among others, Apple scored a one.

In the marriage measure, for instance, Apple was cited for supporting same-sex marriage. The site also gave Apple low marks for being a corporate supporter of Center for American Progress, "a liberal think tank" that "supports abortion as an equal right for women."

There's even a button on the site said to direct site visitors to e-mail Apple CEO Tim Cook directly.

Get Data Sheet, Fortune*'s technology newsletter*

Google

It's a similar story for Google (GOOG, -0.49%), which earned the lowest-possible one out of five from 2ndVote.

The site criticized Google for matching gifts to the Brady Campaign, an effort that 2ndVote says opposes "Stand Your Ground laws and concealed carry."

In its discussion on the environment, 2ndVote says Google "engages with the World Wildlife Fund, which is an organization that supports a carbon tax and also supports the 2015 Paris climate deal."

Microsoft

Microsoft (MSFT, -0.31%) also couldn't break from its competitors and ultimately scored a one out of five in the 2ndVote test.

Microsoft is another supporter of the Brady Campaign, which earned it low marks on 2nd Amendment rights. The tech giant was also hit for being "a partner of The Nature Conservancy, a liberal and active proponent of cap-and-trade and a carbon tax."

In its evaluation of Microsoft, 2ndVote also says that the company supports organizations, like Center for American Progress and the League of United Latin American Citizens, which support sanctuary cities.

Samsung

Not even the Korea-based Samsung (SSNLF, +242224.56%) could sidestep a 2ndVote rating. And like many others in the technology space, Samsung received a one out of five from 2ndVote.

Interestingly, 2ndVote didn't have much to say about Samsung. While other companies were tapped for having relationships with multiple "liberal" organizations, Samsung's score was based on its support for one organization: the Center for American Progress.

From the 2nd Amendment to religious liberty, it was Samsung's support for the Center that earned it just one point in all the metrics. No other evidence was cited by 2ndVote, nor were other organizations with which Samsung might be involved.

Center for American Progress

Our Supporters

The Center for American Progress' work is supported by generous donors and partners—including individuals, foundations, corporations, and other organizations—that share the Center's mission and objectives. We are proud to recognize the following supporters that gave $5,000 or more to further the Center for American Progress' work during 2017.

The Center for American Progress receives more than 92 percent of its charitable contributions from individuals and foundations. Corporate funding comprises less than 3 percent of the budget, and foreign government funding comprises only 2 percent.

Our policy work is independent and driven by solutions that we believe will create a more equitable and just country. Corporate donors are not permitted to remain anonymous and corporate donations do not fund new research.

$1,000,000 or more

Anonymous (5)
Democracy Forward
Fidelity Charitable Gift Fund
Ford Foundation
Bill & Melinda Gates Foundation
The William and Flora Hewlett Foundation
The Hutchins Family Foundation
W.K. Kellogg Foundation
Jonathan and Jeannie Lavine Family Fund
Open Society Foundations

Sandler Foundation

TomKat Charitable Trust

$500,000 to $999,999

Anonymous (2)

Carnegie Corporation of New York

Embassy of the United Arab Emirates

Amy P. Goldman Foundation

Joyce Foundation

John D. and Catherine T. MacArthur Foundation

National Philanthropic Trust

The David and Lucile Packard Foundation

The Rockefeller Foundation

Siegel Family Endowment

Silicon Valley Community Foundation

Walton Family Foundation

$100,000 to $499,999

Anonymous (4)

American Federation of State, County and Municipal Employees (AFSCME)

Apple Inc.

The Arcus Foundation

Stewart Bainum Jr.

Bloomberg Philanthropies

Paul Boskind

William K. Bowes, Jr. Foundation

The California Endowment

Annie E. Casey Foundation

Consolidated Contractors Company

Quinn Delaney and Wayne Jordan

Blair Effron

Paul & Joanne Egerman Family Charitable Foundation

Dr. Anita Friedman

First Five Years Fund

Foundation for the Greatest Good
Mark Gallogly and Lise Strickler
Gill Foundation
Goldman-Sonnenfeldt Foundation
H&R Block
Hagedorn Foundation
Irving Harris Foundation
Heising-Simons Foundation
HR&A Advisors
The Kendeda Fund
The Kresge Foundation
Lumina Foundation
Mai Family Foundation
Microsoft Corporation
Eric Mindich
New Venture Fund
New York Community Trust
Open Philanthropy Project
Robert W. Roche
Robert E. Rubin
Schlosstein-Hartley Family Foundation
Stephen M. Silberstein Foundation
Stiftung Mercator
Vanguard Charitable Endowment Program
The WhyNot Initiative

$50,000 to $99,999

Anonymous (5)
444S Foundation
Robert Abernethy
American Federation of Teachers (AFT)
William and Bonnie Apfelbaum
AT&T
Bank of America

The Bauman Foundation

Blackstone

Campion Foundation

CareFirst BlueCross BlueShield

Coalition for Public Safety

Common Counsel Foundation

Covanta

Embassy of Japan

Marc Fasteau and Anne G. Fredericks

Google

Sanjay Govil

Evelyn & Walter Haas, Jr. Fund

The Nick and Leslie Hanauer Foundation

Fred P. Hochberg and Thomas P. Healy

James Hormel

Infinite Computer Solutions Inc.

Tony James

Johnson Family Foundation

Altman Kazickas Foundation

LaSalle Adams Fund

Dale P. Mathias

Rebecca and Nathan Milikowsky

Ken Miller and Lybess Sweezy

Rockefeller Family Fund

Schwab Charitable Fund

Taipei Economic and Cultural Representative Office in the United States, or TECRO

United Minds for Progress

Henry van Ameringen

Jon F. Vein

Wallace Global Fund

Walmart

Wilburforce Foundation

$5,000 to $49,999

Anonymous (14)
A. L. Mailman Family Foundation
Wendy and Jim Abrams
ADARA Charitable Fund
Madeleine K. Albright
The Albright Stonebridge Group
American Association for Justice (AAJ)
American Beverage Association
The American Express Company
Greg and Anne Avis
Bank of America Charitable Gift Fund
B.W. Bastian Foundation
Nina Beattie and Michael Eberstadt
Carol and Frank Biondi
Adam Blumenthal
Brownstein Hyatt Farber Schreck, LLP
C.J.L. Charitable Foundation
California Community Foundation
James Capalino
Capricorn Management, LLC
Chan Zuckerberg Initiative
Dana Chasin
Simon Clark
Steven Cohen
David Colden
Combined Federal Campaign
Connecticut Street Foundation
CVS Health
Raj Date
Defenders of Wildlife
Discovery Communications
Eileen Donahoe
East Bay Community Foundation
Charles Leonard Egan

Elmo Foundation

Everytown for Gun Safety Action Fund

Express Scripts

Facebook

Federal Foreign Office of the Federal Republic of Germany

Joseph and Marie Field Foundation

Geoffrey Garin

General Electric

Heinrich Böll Foundation

Ann and Gordon Getty Foundation

Lisa and Douglas Goldman Fund

William Goldman

Joshua Greer

Garrett Gruener and Amy Slater Family Fund

Estate of Vincent Gulisano

Margaret and Shashi Gupta

Craig and Kathryn Hall

Heinrich-Böll-Stiftung North America

Joe Henderson

The Heyday Foundation

Belle Horwitz and Jonathan Weiner

Institute of International Education

Invariant

Joan and Irwin Jacobs

Japan Bank for International Cooperation

Jewish Community Foundation

Michael W. Kempner

Ed Kissam

Lebowitz-Aberly Family Foundation

Lefkofsky Family Foundation

Leonardo DRS

Damon & Heidi Lindelof

Hani Masri

Master Your Card

James Mauch

McLarty Associates

The Herbert McLaughlin Children's Trust

Al Mottur

Kristin Mugford

The Philip and Tammy Murphy Family Foundation

Nicole Mutchnik

MWW

Shekar Narasimhan

New Silk Route Advisors LP

Joyce Newstat and Susan Lowenberg

NVG LLC

Peter Orszag

Pacific Gas and Electric Company

Alan Patricof

Pearson Education

PepsiCo Inc.

Anne Peretz

Peter G. Peterson Foundation

Andrew Pincus

Heather Podesta

Portlight Inclusive Disaster Strategies

The Pritzker Children's Initiative

Quest Diagnostics

Deepak Raj

Steven Rattner and Maureen White

Robert Raymar

Francene and Charles Rodgers

Marti and Greg Rosenbaum

Laura Ross

Samsung

Parag Saxena

Alan & Susan Lewis Solomont Family Foundation

The Summers/New Family

Temasek

The Travelers Indemnity Company

Trehan Foundation Inc.
Tom and Janet Unterman
Philippe and Katherine Villers
Jeffrey C. Walker
Hope Warschaw
Herbert S. Winokur Jr
Robert Wolf

If you would like to make a gift to the Center for American Progress, please visit our donation page or contact the Development team at 202-481-8185.

Our previous supporters:

- 2016
- 2015
- 2014
- 2013

CIVIL
OKANOGAN COUNTY SUPERIOR COURT
Case Information Cover Sheet (CICS)

Case Number_____ **Case Title** James M. Miller v. Secretary of State, Kim Wyman

Attorney Name James M. Miller, Pro Se **Bar Membership Number** N/A

Please check one category that best describes this case for indexing purposes. Accurate case indexing not only saves time in docketing new cases, but helps in forecasting needed judicial resources. Cause of action definitions are listed on the back of this form. Thank you for your cooperation.

☐	ABJ	Abstract of Judgment	☐	PRG	Property Damage – Gangs
☐	ALR	Administrative Law Review	☐	PRP	Property Damages
☐	ALRJT	Administrative Law Review-Jury Trial (L&I)	☐	QTI	Quiet Title
☐	CRP	Petition for Certificate of Restoration of Opportunity	☐	RDR	Relief from Duty to Register
☐	CHN	Non-Confidential Change of Name	☐	RFR	Restoration of Firearm Rights
☐	COL	Collection	☐	SDR	School District-Required Action Plan
☐	CON	Condemnation	☐	SPC	Seizure of Property-Commission of Crime
☐	COM	Commercial	☐	SPR	Seizure of Property-Resulting from Crime
☐	DOL	Appeal Licensing Revocation	☐	STK	Stalking Petition
☐	DVP	Domestic Violence	☐	SXP	Sexual Assault Protection
☐	EOM	Emancipation of Minor	☐	TAX	Employment Security Tax Warrant
☐	FJU	Foreign Judgment	☐	TAX	L & I Tax Warrant
☐	FOR	Foreclosure	☐	TAX	Licensing Tax Warrant
☐	FPO	Foreign Protection Order	☐	TAX	Revenue Tax Warrant
☐	HAR	Unlawful Harassment	☐	TMV	Tort – Motor Vehicle
☐	INJ	Injunction	☐	TRJ	Transcript of Judgment
☐	INT	Interpleader	☐	TTO	Tort – Other
☐	LCA	Lower Court Appeal – Civil	☐	TXF	Tax Foreclosure
☐	LCI	Lower Court Appeal – Infractions	☐	UND	Unlawful Detainer – Commercial
☐	LUPA	Land Use Petition Act	☐	UND	Unlawful Detainer – Residential
☐	MAL	Other Malpractice	☐	VAP	Vulnerable Adult Protection Order
☐	MED	Medical Malpractice	☐	VVT	Victims of Motor Vehicle Theft-Civil Action
☐	MHA	Malicious Harassment	☐	WDE	Wrongful Death
☐	MSC2	Miscellaneous – Civil	☐	WHC	Writ of Habeas Corpus
☐	MST2	Minor Settlement – Civil (No Guardianship)	☐	WMW	Miscellaneous Writs
☐	PCC	Petition for Civil Commitment (Sexual Predator)	X	WRM	Writ of Mandamus
☐	PFA	Property Fairness Act	☐	WRR	Writ of Restitution
☐	PIN	Personal Injury	☐	WRV	Writ of Review
☐	PRA	Public Records Act	☐	XRP	Extreme Risk Protection Order

IF YOU CANNOT DETERMINE THE APPROPRIATE CATEGORY, PLEASE DESCRIBE THE CAUSE OF ACTION BELOW.

Please Note: Public information in court files and pleadings may be posted on a public Web site.