

From: [Richard Akiona](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Hawaii Elections Commision Testimony
Date: Wednesday, September 14, 2022 10:04:34 AM

I am writing to ask the commission to do your job and correct the way voting is done in Hawaii. Voting should only be done in person. Anyone with common sense will know the amount of fraud that is being done thru mail in voting. Long story short for the record I oppose the software currently being used for Hawaii voting.

Mahalo for your time Richard Akiona (808) 329 5662

From: [Tom Stanton](#)
To: [OE.Elections](#)
Cc: [Ana Mohamad](#); [Laura Nakanelua](#)
Subject: [EXTERNAL] Written Testimony for September 16 Election Commission Meeting
Date: Wednesday, September 14, 2022 8:07:17 PM
Attachments: [2022 Kauai Election Discrepancy.pdf](#)
[2020 Kauai Discrepancies Report.pdf](#)

Dear State of Hawaii Elections Commission,

Please see the attached testimony that I would like to submit to the Elections Commission for the September 16, 2022 meeting. The first pdf is a summary of the Kauai Elections Division chain of custody problem that occurred with the 2022 Kauai Primary Election where documentation for 1905 ballot envelopes has been admitted to being "misplaced". The second pdf summarizes a second Chain of Custody problem that occurred with the Kauai Elections division for the 2020 General Election where 3379 ballot envelopes can not be accounted for. This is in addition to another problem with the Kauai Elections Division chain of custody records for the 2020 Primary Election Drop Box records.

These issues were all recently discovered by a member of the Kauai Board of Registration.

I would greatly appreciate your attention to these matters. I would also like to request time to give oral testimony at September 16, 2022 meeting.

Sincerely,

Thomas Stanton
Hawaii Republican Party District 15 Chair
Kauai Election Integrity Chair
858-344-5413

2022 Kauai Election Discrepancy

On July 29, 2022 Ralph Cushnie from the Kauai Board of Registration requested the following from the Kauai Elections Division:

“Lyndon and Jade please provide a daily auditable accounting of Ballots received from Registered Voters via drop box and USPS for the 2022 Primary Election. The list should include but not limited to:

Daily number of ballots received from each drop location and total ballots received per day from the USPS.

Daily USPS receipt of ballots delivered, and the County verification of daily USPS ballot counts with proper chain of custody forms.

Number of ballots determined to be from non-Registered Voters and therefore will not be counted.

Numbers should be tallied to a summary spread sheet and be auditable to chain of custody records for each drop box location and daily USPS deliveries.

Drop Box plus USPS plus in person voting equal State of Hawaii official results

I look forward to working with you both and to help with your continued efforts to ensure safe and secure elections.”

(Mr Yoshioka replies are in red. My personal comments are in blue)

On August 4, 2022 Mr. Yoshioka replied to Mr. Cushnie with the follow chart and said:

“Current ballot envelope manual hand-counts are depicted below. Envelopes from the different sources were mixed up on 7/28 and 7/29 so only a total is reported. However, the bulk did come from the USPS. As stated previously these manual counts are only used to gauge work flow and resource allocation.”

In addition to the problems documented in my previous summary with the 2020 Primary Election Drop Box lack of Chain of Custody records and the 2020 General Election discrepancy for Ballots Envelopes received there is now a problem with the 2022 Kauai Elections Division Chain of custody for Drop Box and USPS Ballot Envelopes received. This time for 1905 Ballot Envelopes received on 7/28/2022 and 7/29/2022. Mr. Yoshioka states that the “bulk did come from USPS” but there is no additional documentation provided to confirm this. There should be no ambiguity about these numbers because there is a clear procedure in place for drop box chain of custody logs and delivery logs from the USPS. I was told first hand by the ballot transport observers and election division personnel that logs are kept for the drop box and USPS deliveries. Mr Yoshioka then goes on to emphasize that “these manual counts are only used to gauge work flow and resource allocation”. Why can't Mr. Yoshioka and the Kauai Elections Division simply produce the actual logs for the Ballot Envelopes delivered to them? This is a simple chain of custody issue.

Date	Hanalei NC	Princeville Library	Kilauea NC	Waipouli SC	Elections Division	Kōloa NC	Kalāheo NC	Hanalei NC	Waimea NC	USPS	Office	VSC	
7/28/22													843
7/29/22													1,082
7/30/22	0	0	2	1	26	2	3	1	4	851	0	0	890
8/2/22	3	4	0	7	62	2	1	0	1	778	12	4	874
8/3/22	0	0	0	0	53	0	0	0	0	1,084	12	0	1,149

On August 24, 2022 Mr. Cushnie asked for the final Kauai ballot received numbers for the 2022 Primary Election and received the following response and chart from Mr Yoshioka.

"The updated counts are below. As stated previously these rough manual counts that are only used to gauge work flow and to assist in allocating resources."

"Additionally, please note the following:

The "No. Pulled" column represents the number of envelopes that were pulled for the day because they were unsigned or contained a non-matching signature;

The "Received Manually" column represents the number of envelopes that were added back into the count because the envelope issue (i.e., missing or non-matching signature) which initially caused the envelope to be pulled was cured by the voter (i.e., signed and signature verified); and

Individual counts for 7/28/22 and 7/29/22 were misplaced so only the Total is provided for those dates."

Mr Yoshioka States again that the numbers he is providing are "rough manual counts that are only used to gauge work flow and assist in allocating resources". As with Mr. Cushnie's 2020 inquiries why is Mr. Yoshioka only providing "rough counts" of the ballots received? He also states that the records for individual counts for 7/28/22 and 7/29/22 were "misplaced" so only the total is provided. Please note in Mr. Yoshioka's first reply he states the envelopes from the different sources were "mixed up" now he states that the records are "misplaced".

Date	Hanalei NC	Princeville Library	Kilauea NC	Waipouli SC	Elections Division	Kōloa NC	Kalaheo NC	Hanalei NC	Waimea NC	USPS	Office	VSC	Subtotals	No. Pulled	Received Manually	Total
7/28/22																843
7/29/22																1,062
7/30/22	0	0	2	1	26	1	3	1	4	851	0	0	890	19	0	871
8/2/22	3	4	0	7	62	2	1	0	1	778	12	4	874	22	0	852
8/3/22	0	0	0	0	53	0	0	0	0	1,084	12	0	1,149	32	3	1,120
8/4/22	1	5	1	3	42	1	1	5	5	980	7	0	1,051	32	4	1,028
8/5/22	0	0	0	0	36	0	0	0	0	973	2	0	1,011	18	22	1,015
8/8/22	0	4	8	3	47	0	10	4	2	662	9	0	749	22	12	759
8/9/22	0	11	8	7	130	6	6	0	1	720	20	0	809	20	35	824
8/10/22	0	7	16	8	115	6	9	1	5	0	28	0	190	3	7	194
8/11/22	3	7	15	18	180	7	10	20	7	2,012	11	5	2,295	67	62	2,280
8/12/22	7	31	30	30	277	23	42	14	17	1,101	18	12	1,602	22	111	1,691
8/13/22	6	32	32	36	310	21	38	26	14	823	34	0	1,372	0	54	1,426
8/13/22	0	0	0	0	220	0	0	0	0	0	0	0	220	25	0	195
8/13/22	0	0	0	0	309	0	0	0	0	630	46	10	995	0	0	995
8/23/22	0	0	0	0	617	0	0	0	0	708	29	41	1,395	0	0	1,395
8/13/22	0	0	0	0	0	0	0	0	0	0	0	0	0	29	50	21
8/13/22	48	103	133	138	0	117	187	88	82	0	0	0	996	0	0	996
TOTALS	68	204	245	351	2,424	185	307	150	138	11,322	223	72	15,668	311	360	17,652

On August 30, 2022 Mr. Cushnie asked how the 2020 Primary Election could be certified without proper chain of custody for 1905 ballots.

Good morning, Lyndon, and Jade, thank you again for helping me understand the election process. As it relates to counts on 7-28-22 and 7-29-22 there are 1905 ballots that do not have chain of custody documentation. How will the election get certified especially county council races with out this information? How do we know where these ballots came from? How can ballots be received at the county election center with no inventory control and missing chain of custody documents. I would not anticipate that these would be minor details that can be overlooked or be optionable. Is there a flow diagram that you work with or rules explaining how this is allowed? Thank you for your patience.

As of 9/3/2022 Mr. Cushnie has not received an answer as to how the Kauai Elections Division or the Hawaii Office of Elections was able to certify the Kauai election results with 1905 ballots not having proper chain of custod

How can the Kauai Elections Division certify the 2022 Primary Election results if they do not have chain of custody records for the 1905 ballot envelopes that were received on 7/28/2022 and 7/29/2022? Mr Yoshioka has admitted the records for 7/28/2022 and 7/29/2022 are "misplaced" and that the other ballot received numbers he provided to the Kauai Board of Registration are only "rough manual counts".

If anyone has questions about this report please contact Tom Stanton at stantonproperties@sbcglobal.net or Ralph Cushnie at ralph@cushniecci.com.

Tom Stanton
KRP District 15 Chair
858-344-5413

2020 Kauai Election Ballot Count Discrepancy

On July 12, 2022 Ralph Cushnie from the Board of Registration asked Lyndon Yoshioka at the Kauai Elections Division for the 2020 Received Ballot Envelope numbers.

On July 14, 2022 Lyndon Yoshioka replied and attached several documents which included the following summary with totals for drop box locations and the USPS ballots envelopes received.

(Mr Yoshioka replies are highlighted in red. My personal comments are in blue. Aulii Ten's reply, the head of counting center operations on Oahu, are in pink).

"See attached. We could not locate Dropbox counts for the 2020 Primary Election."

(This means there is no chain of custody for any of ballots that came from the drop boxes for 2020 Primary Election. There should be Drop Box transport logs for these ballots).

2020 GENERAL ELECTION DROPBOX COUNTS

ELECTIONS OFFICE/WINDOW	821
ELECTIONS OFFICE/DROP BOX	1977
HANAIEI FIRE STATION	539
HANAIEI NEIGHBORHOOD CENTER	116
HANAPEPE FIRE STATION	238
KALAHEO FIRE STATION	492
KAPAA FIRE STATION	797
KILAUEA NEIGHBORHOOD CENTER	272
KOLOA NEIGHBORHOOD CENTER	363
USPS	20929
VOTER SERVICE CENTER	1573
WAIMEA NEIGHBORHOOD CENTER	235

The above numbers provided by the Kauai Elections Division shows the totals for the ballot envelopes picked up at each drop box location and the U.S.P.S. mail in ballot envelopes received by the Kauai election division. The total for all ballot envelopes received (which is not displayed) is 28,352 with 20,929 coming from USPS and 7423 coming from the various Drop Box locations.

When Mr. Cushnie compared these numbers to the Kauai Summary Report (See below) he found a discrepancy. The total on the state report for all drop box and mail in ballot envelopes received was 31,731.

This is a difference of 3379 additional ballots which is approximately 10% of all the Ballots Received.

President and Vice President			Councilmember, County of Kauai		
(D) BIDEN / HARRIS	21,225	82.3%	Number To Vote For: 7		
(R) TRUMP / PENCE	11,582	34.0%	CHOCK, Mason K.	18,599	7.8%
(L) JORGENSEN / COHEN	303	0.9%	EVSUN, Luke A.	17,371	7.3%
(G) HAWKINS / WALKER	254	0.7%	KANESHIRO, Amyl	16,555	6.9%
(AS) PIERCE / BALLARD	77	0.2%	CARVALHO, Bernard, Jr.	16,351	6.9%
(C) BLANKENSHIP / MOHR	56	0.2%	DecOSTA, Billy	14,523	6.1%
Blank Votes	559	1.6%	COWDEN, Felicia	14,394	6.0%
Over Votes	25	0.1%	KUALIE, Kipuka L. P.	13,964	5.9%
U.S. Representative, Dist II			BULOSAN, Addison	11,744	4.9%
(D) KAHELE, Kaieli (Kai)	19,880	56.3%	WAIKALEA BATTAD, Jade T.	11,002	4.6%
(R) AKANA, Joe	8,233	24.2%	JUSTUS, Ed	8,601	2.8%
(A) HOOMANAWANUI, Jonathan	812	2.4%	DANDURAND, Mike	6,283	2.6%
(L) TIPPENS, Michelle Rose	582	1.7%	NISHIMURA, Wally K.	6,213	2.6%
(N) BURRUS, Ron	182	0.5%	SIMBRE-MEDEIROS, Shirley R.	5,650	2.4%
(AS) GIUFFRÉ, John (Raghu)	35	0.1%	FUKUSHIMA, Richard S.	5,038	2.1%
Blank Votes	4,330	12.7%	Blank Votes	74,025	31.0%
Over Votes	27	0.1%	Over Votes	36	0.1%
State Representative, Dist 14			KAUA'I: Negligence Claims		
(D) NAKAMURA, Nadine K.	7,983	69.7%	YES	23,350	68.5%
(R) MONAS, Steve	2,430	21.7%	NO	5,330	15.6%
Blank Votes	978	8.5%	Blank Votes	5,394	15.8%
Over Votes	2	0.0%	Over Votes	7	0.0%
State Representative, Dist 15			KAUA'I: Police Chief Qualifications		
(D) TOKIOKA, James Kunene	7,712	86.7%	YES	24,351	71.5%
(R) YODER, Steve	2,880	24.9%	NO	8,342	18.6%
Blank votes	965	8.3%	Blank Votes	3,378	9.9%
Over Votes	6	0.1%	Over Votes	10	0.0%
State Representative, Dist 16			KAUA'I: Ethics Disclosures		
(D) MORIKAWA, Daynette (Dee)	7,329	86.2%	YES	26,398	77.5%
(R) DES, Ana Mo	2,511	23.5%	NO	3,402	10.0%
Blank votes	1,121	10.1%	Blank Votes	4,274	12.5%
Over Votes	4	0.0%	Over Votes	7	0.0%
Hawaii Resident Trustee			KAUA'I: Prosecutor Vacancy		
LINDSEY, Keola	10,817	31.7%	YES	23,861	70.0%
MANGAUL, Lanihale	6,597	19.7%	NO	5,618	16.5%
Blank Votes	15,562	46.6%	Blank Votes	4,595	13.5%
Over Votes	5	0.0%	Over Votes	9	0.0%
Molokai Resident Trustee			KAUA'I: County Engineer Qualifications		
ALAPA, Luana	8,385	24.8%	YES	21,079	61.8%
MACHADO, Colette (Pipi)	7,503	23.2%	NO	8,733	25.6%
Blank Votes	17,789	52.2%	Blank Votes	4,244	12.5%
Over Votes	4	0.0%	Over Votes	25	0.1%
At-Large Trustee			KAUA'I: Water Board Manager Qualifications		
AKINA, Ke'li	9,153	26.9%	YES	21,073	61.8%
SOUZA, Keoni	9,118	26.8%	NO	8,748	25.7%
Blank Votes	15,803	46.4%	Blank Votes	4,251	12.5%
Over Votes	7	0.0%	Over Votes	9	0.0%
REGISTRATION AND TURNOUT			GENERAL		
*****			*****		
TOTAL REGISTRATION			47,253		
TOTAL TURNOUT			51,581 72.1%		
MAIL TURNOUT			31,731 57.2%		
IN-PERSON TURNOUT			2,350 3.0%		

Chain of Custody
30,702 - 3,579
28,352
2,350
↑

Mr. Cushnie asked for an explanation as to why the Kauai Elections Ballots Envelope numbers provided by Mr Yoshioka were different from the final summary report Mr. Yoshioka replied on July 20, 2022 with the following explanation:

"Per your request the counts provided only represent envelopes received via drop boxes, not ballots counted."

(This answer does not explain why the number of received ballots is different on the two reports but implies that the discrepancy is coming from additional ballots being counted).

Mr. Cushnie then asked for an additional explanation for the discrepancy and how the ballot chain of custody was handled and was told on July 23, 2022 by Mr. Yoshioka:

"Voted ballot envelope chain of custody:

Voter > USPS > Election Division

Voter > Dropbox > Election Division

Voter > Election Division (in-person drop-off at service window)"

"The discrepancy is likely due to inaccurate manual envelope counts over time. I will check with staff and get back to you."

This would mean over the two week time of the election the elections division incorrectly counted 10% of all ballots received. I do not believe this is reasonable because I personally observed how seriously the ballot chain of custody is taken by all the election workers and volunteers. The ballot chain of custody procedure is also very specific as referenced in the County of Kauai Place of Deposit Collection Procedure Manual and Counting Center Manual.*Attached.

On July 24, 2022 Mr. Cushnie asked if the discrepancy could have been a problem with the counting machines and Mr. Yoshioka follow up email stated:

"The counts taken were intended to provide our office with a rough number of envelopes received so we could estimate the number of outstanding envelopes and use this count to properly allocate resources. To imply that a discrepancy in this count and the number of ballots counted is a sign that something nefarious has occurred is wrong."

Again this does not explain the discrepancy. More importantly why would the elections division give out rough estimates of the ballot envelopes received when asked for the official 2020 ballot numbers? There are logs for Ballots Envelopes received from the drop boxes and the USPS. The elections division should simply produce the ballot transfer logs and/or the USPS delivery logs? That would easily have put this matter to rest.

The Kauai Elections Division then forwarded Mr. Cushnie's questions to the Hawaii Office of Elections and on August 1, 2022 Mr. Cushnie received an email from Aulii Tenn the Head of Counting Center Operations:

Dear Mr. Cushnie,

The County of Kauai has forwarded us your questions concerning the counting of ballots as our office is statutorily responsible for such matters. With that in mind, below are our responses to your questions:

At what stage are the envelopes separated from the ballots?

Return identification envelopes containing the ballots are transferred to the counting center. Once at the counting center, ballots may commence being separated from the return identification envelopes. HRS § 11-108.

If envelopes received plus in person votes is less than ballots reported how were the remaining ballots matched to the registered voter list?

What you are referring to is an overage. This occurs when there are "more ballots than documented usage indicates." An underage, in contrast, occurs when there are fewer ballots. Both circumstances are documented by officials. There is no exhaustive list of how an overage or underage can occur.

Please note that election officials review whether there is a pattern in relation to the overages or underages that could indicate fraud or a

significant operational issue and will take appropriate steps depending on what the pattern indicates.

Aloha,
Aulii Tenn
Counting Center Operations

Mrs. Tenn's response again does not give a satisfactory answer as to why there is a difference in the documented ballot envelope numbers and the final summary report but simply says it is an "overage" which "occurs when there are more ballots than documented usage indicates". She then goes on to say "Please note that election officials review whether there is a pattern in relation to the overages or underages that could indicate fraud or a significant operational issue and will take appropriate steps depending on what the pattern indicates."

On August 1, 2020 Mr. Cushnie replied to Aulii Ten and ask if she could provide any chain of custody for the 3379 ballots that were recorded on the final summary report. As of 9/3/2022 Mr. Cushnie has not received an answer as to how the 3379 difference in ballot envelopes received has been reconciled or if there is proper chain of custody for the 2020 Ballot Envelopes received by the Kauai Elections Division.

If anyone has questions about this report please contact Tom Stanton at stantonproperties@sbcglobal.net or Ralph Cushnie at ralph@cushniecci.com.

Tom Stanton
KRP District 15 Chair
858-344-5413

From: [Laura Nakanelua](#)
To: [OE.Elections](#)
Cc: [Kataoka, Jaime N](#)
Subject: [EXTERNAL] Fwd: Signed letter to OE
Date: Thursday, September 15, 2022 11:02:20 AM
Attachments: [Scheduling Request Elections Commission 220914_195412.pdf](#)

Aloha,

Please find attached letter from HI GOP Chair Lynn Finnegan.

Kindly forward a copy to Elections Commissioners and include in meeting materials for the 9/16 meeting.

Mahalo,
Laura



Laura Nakanelua
National Committeewoman, Hawai'i
Republican National Committee
C: (808) 561-2325

----- Forwarded message -----

From: Lynn Finnegan, State Chair <lynn@gophawaii.com>
Date: Wed, Sep 14, 2022 at 9:21 PM
Subject: Signed letter to OE
To: Laura Nakanelua <lauranakanelua@gmail.com>

Mahalo!
Lynn Finnegan
State Chair
Hawai'i Republican Party
C: 808-741-5966

Sent from my iPhone



September 14, 2022

Hawai'i Republican Party
725 Kapiolani Blvd. #C-105
Honolulu, HI 96813

Mr. Scotty Anderson
Elections Commission
c/o Office of Elections
802 Lehua Avenue
Pearl City, Hawaii 96782

Dear Chair Anderson,

It has been brought to my attention that the Office of Elections has scheduled a meeting of the Elections Commission on September 16th at 10am, when Commissioner Lillian Koller is not allowed to participate due to her employment. Commissioner Koller sent an email back to Jaime Kataoka as soon as she received the notice of the meeting and stated that she could not miss work in order to attend the meeting. Ms. Kataoka replied "that day was the day that had the best availability amongst the Commissioners. However, it is a tentative date at this time; I will keep you posted with any changes."

Ms. Koller immediately submitted subsequent requests to have the meeting rescheduled for a time that worked for all Commissioners, and also made it known that she could participate later in the afternoon of the 16th but received no response at all from Ms. Kataoka.

Our Hawai'i Elections Commission is intended to be a balanced, bi-partisan body of citizens who work on behalf of the people of Hawaii to hold public hearings for the purposes of receiving evidence of any violations and complaints relative to our elections in Hawaii and, if necessary, to investigate that evidence as well as advise the Chief Election Officer on matters relating to elections.

Scheduling the EC meetings should not be a matter of what's most convenient for the Commissioners but, rather, what is possible to ensure that all Commissioners can participate and represent the people without impediment. Scheduling the meeting at a time when it is known that one of your Republican-appointed Commissioners cannot participate is unacceptable.

No Commissioner should be required to "pay" to participate in EC meetings by forfeiting work. This is a matter of principle. The EC Commissioners are specifically selected and approved to participate on the Commission and none of them should be asked to choose between their civil service and employment.

Kindly consider rescheduling the meeting to a time that works for all Commissioners.

Respectfully,



Lynn Finnegan
State Chair
Hawaii Republican Party
C: 808-741-5966



September 16, 2022

Dear Members of the Election Commission and Scott Nago,

I am unable to attend the Election Commission meeting this morning but have a few comments that I would like to submit. Because of my last minute submission of these comments, is it possible for them to be read? If not, they will be testimony to my views as a citizen of Hawaii.

On your website, it says that the Office of Election's mission is: "to provide secure, accessible and convenient election services to all citizens of Hawaii".

I want to address the "secure" aspect of election services in our state. In Case no. cv 22 00381 JMS WRP in the United States District Court for Hawaii, Pirtle vs. Nago, two issues regarding "security" of elections are outlined.

One is lack of proper chain of custody procedures. Even though this was proclaimed an issue by the Commission, no follow up occurred. When a state has gone to mail in voting, and there are no proper procedures to guarantee proper chain of custody how could our rights to have our votes counted accurately be secured?

In addition, all voting systems in use in the United States, now and in 2020, are subject to tampering through a Trapdoor mechanism inherent in all election systems. This Trapdoor mechanism is described in detail in Exhibit A, affidavit of Terpsehore Maras, filed under penalty of perjury on December 1, 2020, in case #2:20-cv-01771-PP in the 2nd Judicial District of the Denver District Court in Denver, Colorado.

I have attached this affidavit.

We must go back to pen and paper ballots. People show up in person and cast their votes after showing their ID's. Those who cannot cast their ballot in person, make a request for an absentee ballot.

Our vote is our voice.

Mahalo,

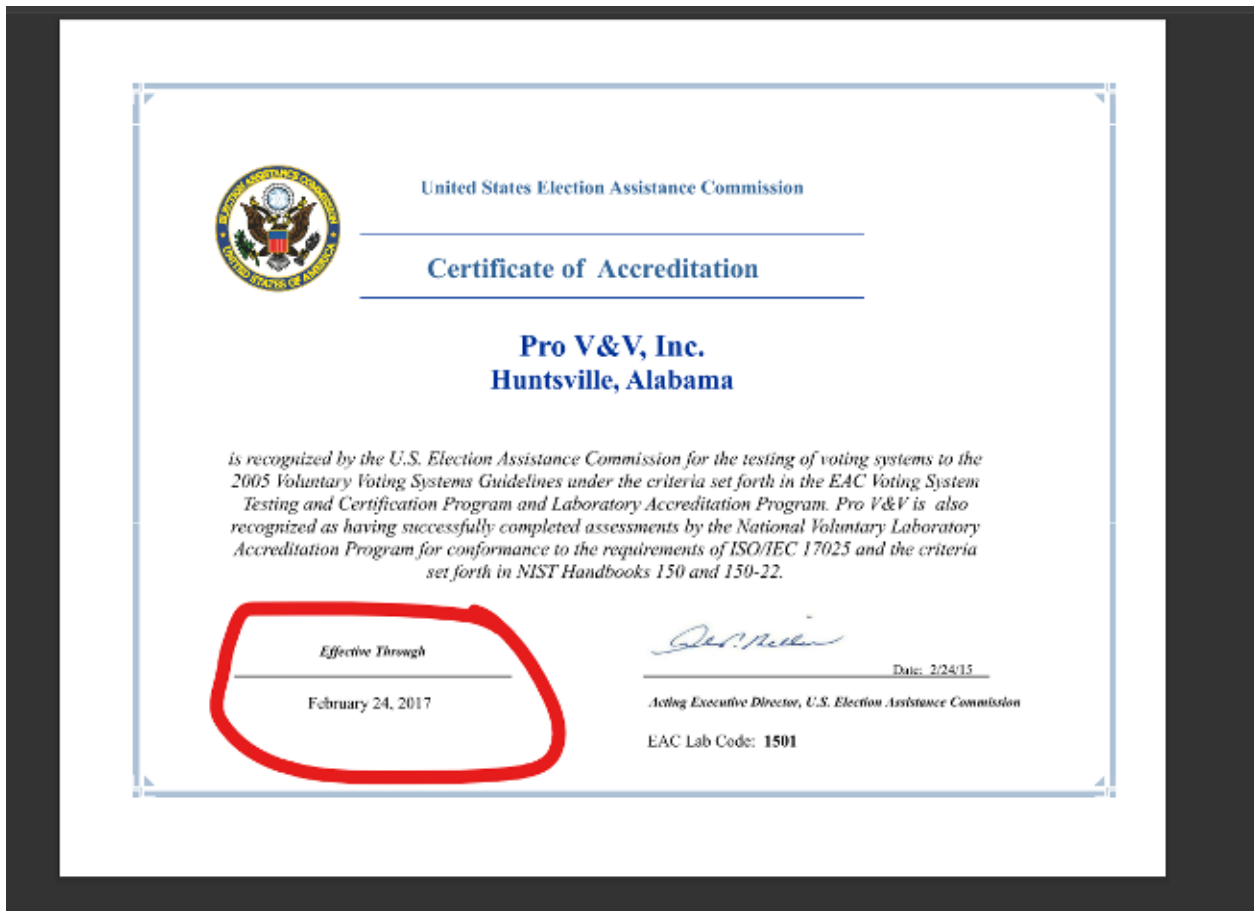
Marina Poling

Declaration of Terpsehore P Maras

Pursuant to 28 U.S.C Section 1746, I, Terpsehore P Maras, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I have been a private contractor with experience gathering and analyzing foreign intelligence and acted as a LOCALIZER during the deployment of projects and operations both OCONUS and CONUS. I am a trained Cryptolinguist, hold a completed degree in Molecular and Cellular Physiology and have FORMAL training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, Predictive Analytics among others.
3. I have operational experience in sources and methods of implementing operations during elections both CONUS and OCONUS
4. I am an amateur network tracer and cryptographer and have over two decades of mathematical modeling and pattern analysis.
5. In my position from 1999-2014 I was responsible for delegating implementation via other contractors sub-contracting with US or 9 EYES agencies identifying connectivity, networking and subcontractors that would manage the micro operations.
6. My information is my personal knowledge and ability to detect relationships between the companies and validate that with the cryptographic knowledge I know and attest to as well as evidence of these relationships.
7. In addition, I am WELL versed due to my assignments during my time as a private contractor of how elections OCONUS (for countries I have had an assignment at) and CONUS (well versed in HAVA ACT) and more.
8. On or about October 2017 I had reached out to the US Senate Majority Leader with an affidavit claiming that our elections in 2017 may be null and void due to lack of EAC certifications. In fact Sen. Wyden sent a letter to Jack Cobb on 31 OCT 2017 advising discreetly pointing out the importance of being CERTIFIED EAC had issued a certificate to

Pro V & V and that expired on Feb 24, 2017. No other certification has been located.



9. Section 231(b) of the Help America Vote Act (HAVA) of 2002 (42 U.S.C. §15371(b)) requires that the EAC provide for the accreditation and revocation of accreditation of independent, non-federal laboratories qualified to test voting systems to Federal standards. Generally, the EAC considers for accreditation those laboratories evaluated and recommended by the National Institute of Standards and Technology (NIST) pursuant to HAVA Section 231(b)(1). However, consistent with HAVA Section 231(b)(2)(B), the Commission may also vote to accredit laboratories outside of those recommended by NIST upon publication of an explanation of the reason for any such accreditation.

United States Department of Commerce
National Institute of Standards and Technology



Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200978-0

Pro V&V
Huntsville, AL

*is accredited by the National Voluntary Laboratory Accreditation Program for specific services,
listed on the Scope of Accreditation, for:*

Voting System Testing

*This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017.
This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality
management system (refer to joint ISO-ILAC-IAF Communiqué dated January 2009).*

2020-03-26 through 2021-03-31
Effective Dates




For the National Voluntary Laboratory Accreditation Program

10.

11. VSTL's are VERY important because equipment vulnerabilities allow for deployment of algorithms and scripts to intercept, alter and adjust voting tallies.
12. There are only TWO accredited VSTLs (VOTING SYSTEM TEST LABORATORIES). In order to meet its statutory requirements under HAVA §15371(b), the EAC has developed the EAC's Voting System Test Laboratory Accreditation Program. The procedural requirements of the program are established in the proposed information collection, the EAC [Voting System Test Laboratory Accreditation Program Manual](#). Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of this Manual will supersede any prior laboratory accreditation requirements issued by the EAC. This manual shall be read in conjunction with the EAC's [Voting System Testing and Certification Program Manual](#) (OMB 3265-0019).



MICHIGAN

<i>State Participation:</i>	Requires Testing by an Independent Testing Authority. MI requires that voting systems are certified by an independent testing authority accredited by NASED and the board of state canvassers.
<i>Applicable Statute(s):</i>	“An electronic voting system shall not be used in an election unless it is approved by the board of state canvassers ... and unless it meets 1 of the following conditions: (a) Is certified by an independent testing authority accredited by the national association of state election directors and by the board of state canvassers. (b) In the absence of an accredited independent testing authority, is certified by the manufacturer of the voting system as meeting or exceeding the performance and test standards referenced in subdivision (a) in a manner prescribed by the board of state canvassers.” MICH. COMP. LAWS ANN § 168.795a (2009).
<i>Applicable Regulation(s):</i>	MI does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State accepts requests from persons/corporations wishing to have their voting system examined. The requestor must pay the Secretary of State an application fee of \$1,500.00, file a report listing all of the states in which the voting system has been approved and any reports that these states have made regarding the performance of the voting system. The Board of State Canvassers conducts a field test involving Michigan electors and election officials in simulated election day conditions. The Board of State Canvassers shall approve the voting system if it meets all of the state requirements. MICH. COMP. LAWS ANN § 168.795a (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://www.michigan.gov/sos/0,1607,7-127-1633_8716_45458---,00.html



WISCONSIN

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. WI requires that its voting systems receive approval from an independent testing authority accredited by NASED verifying that the voting systems meet all of the recommended FEC standards.
<i>Applicable Statute(s):</i>	"No ballot, voting device, automatic tabulating equipment or relating equipment and materials to be used in an electronic voting system may be utilized in this state unless it is approved by the board [of election commissioners]." WIS. STAT. ANN. § 5.91 (West 2009).
<i>Applicable Regulation(s):</i>	"An application for approval of an electronic voting system shall be accompanied by all of the following ... [r]eports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission." WIS. ADMIN. CODE GAB § 7.01 (2009).
<i>State Certification Process:</i>	The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using: (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting system be used in an actual election as a condition of the approval. WIS. ADMIN. CODE GAB §§ 7.01, 7.02 (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://elections.state.wi.us/section.asp?linkid=643&locid=47



GEORGIA

State Participation: **Requires Federal Certification.** GA requires that its voting systems are tested to EAC standards by EAC accredited labs and certified by the EAC.

Applicable Statute(s): “Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any voting machine may request the Secretary of State to examine the machine. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any voting machine previously examined and approved by him or her. Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination; provided, however, that in the case of a request by ten or more electors the examination fee shall be \$ 250.00. The Secretary of State may, at any time, in his or her discretion, reexamine any voting machine.” [GA CODE ANN. § 21-2-324](#) (2008).

Applicable Regulation(s): “Prior to submitting a voting system for certification by the State of Georgia, the proposed voting system’s hardware, firmware, and software must have been issued Qualification Certificates from the EAC. These EAC Qualification Certificates must indicate that the proposed voting system has successfully completed the EAC Qualification testing administered by EAC approved ITAs. If for any reason, this level of testing is not available, the Qualification tests shall be conducted by an agency designated by the Secretary of State. In either event, the Qualification tests shall comply with the specifications of the *Voting Systems Standards* published by the EAC.” [GA. COMP. R. & RES. 590-8-1-.01](#) (2009).

State Certification Process: After the voting system has passed EAC Qualification testing, the vendor of the voting system submits a letter to the Office of the Secretary of State requesting certification for the voting system along with a technical data package to the certification agent. An evaluation proposal is created by the certification agent after a preliminary view of the Technical Data Package and sent to the vendor. Any additional EAC ITA testing identified in the evaluation proposal is arranged by the vendor and the certification agent will perform all other tests identified in the evaluation proposal. The certification agent submits a report of their findings to the Secretary of State. Based on these findings the Secretary of State will make a final determination on whether to certify the voting system. [GA. COMP. R. & RES. 590-8-1-.01](#) (2009).

Fielded Voting Systems: *[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].*
<http://www.sos.georgia.gov/Elections/>



PENNSYLVANIA

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. PA requires that its voting systems are approved by a federally recognized independent testing laboratory as meeting federal voting system standards.
<i>Applicable Statute(s):</i>	"Any person or corporation owning, manufacturing or selling, or being interested in the manufacture or sale of, any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government." 25 PA. CONS. STAT. ANN. Code § 3031.5 (West 2008).
<i>Applicable Regulation(s):</i>	PA does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State examines voting systems, upon request, once the voting systems have received approval by a federally recognized independent testing authority. The person(s) requesting the examination of the voting system are responsible for the cost of the examination. After the examination, the Secretary of State issues a report stating whether or not the voting systems are safe and compliant with state and federal requirements. If the voting systems are deemed safe and compliant by the Secretary of State then the systems may be adopted and approved for use in elections by each county through a majority vote of its qualified electors. 25 PA. CONS. STAT. ANN. Code §§ 3031.5, 3031.2 (West 2008).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://www.votespa.com/HowtoVote/tabid/74/language/en-US/Default.aspx

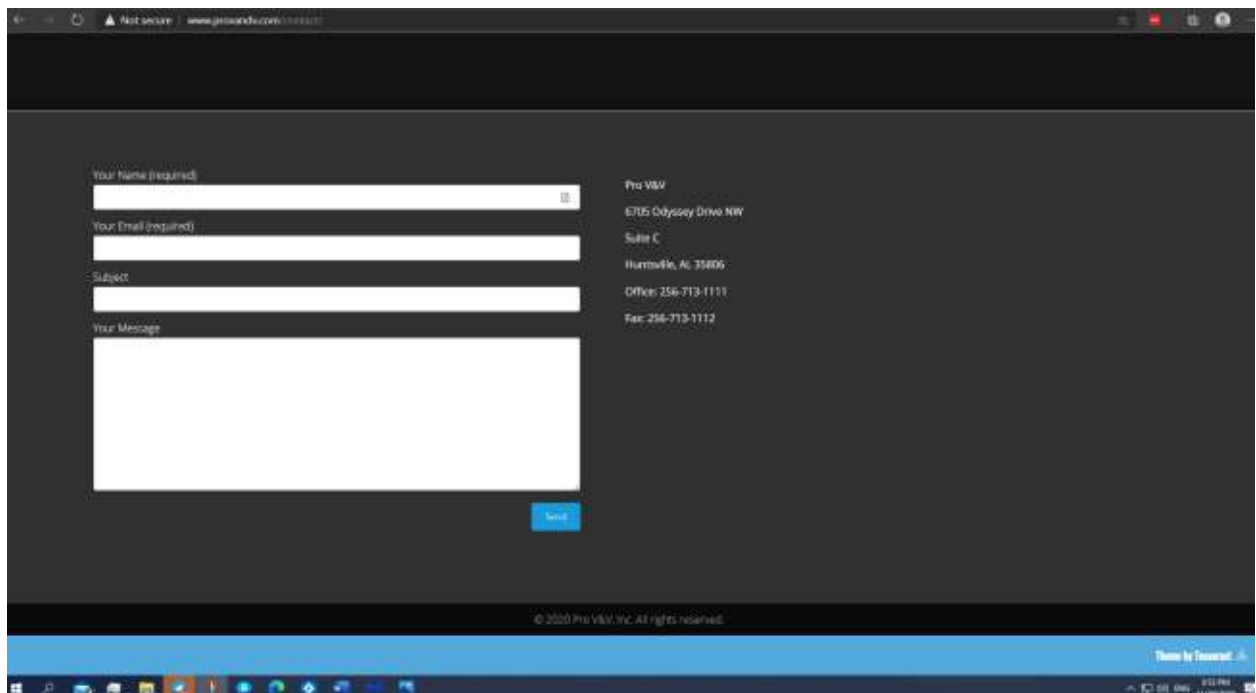
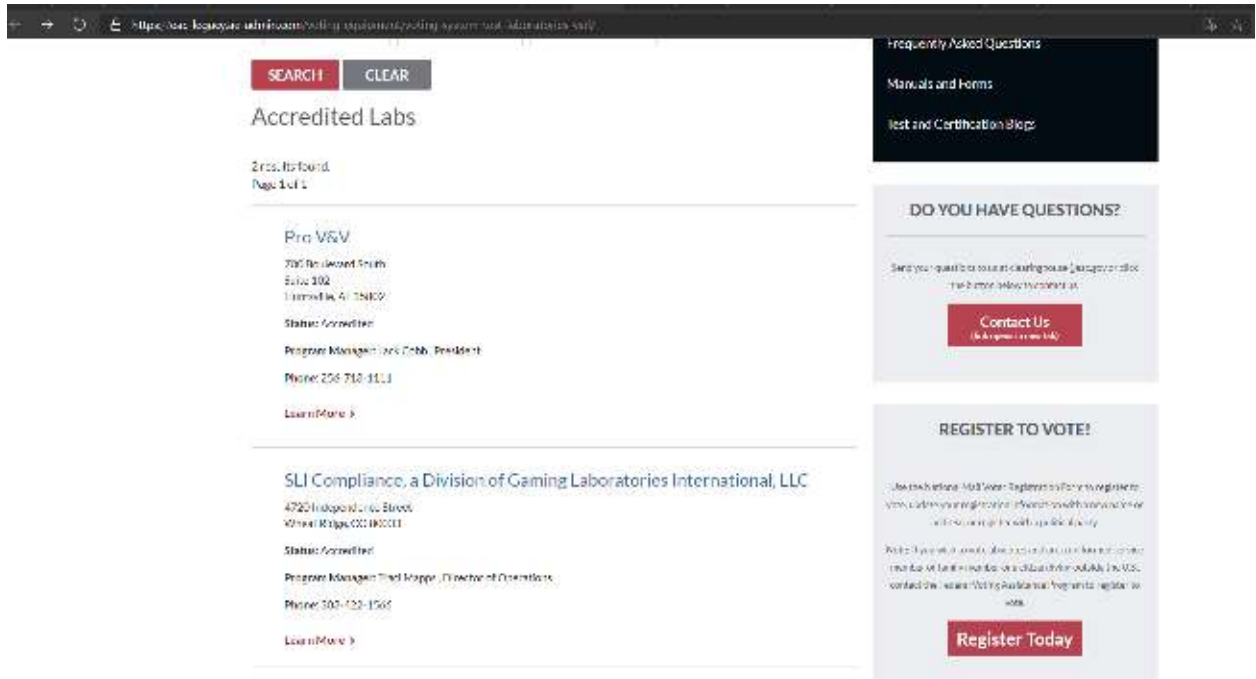


ARIZONA

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. AZ requires that its voting systems are HAVA compliant and approved by a laboratory that is accredited pursuant to HAVA.
<i>Applicable Statute(s):</i>	"On completion of acquisition of machines or devices that comply with HAVA, machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with HAVA and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to HAVA." ARIZ. REV. STAT. § 16-442(B) (2008).
<i>Applicable Regulation(s):</i>	AZ does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State appoints a committee of three people that test different voting systems. This committee is required to submit their recommendations to the Secretary of State who then makes the final decision on which voting system(s) to adopt. ARIZ. REV. STAT. § 16-442(A) and (C) (2008).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://www.azsos.gov/election/equipment/default.htm

- 17.
18. **Pro V& V** and **SLI Gaming** both lack evidence of EAC Accreditation as per the Voting System Testing and Certification Manual.

19. **Pro V&V** is owned and Operated by Jack Cobb. Real name is Ryan Jackson Cobb. The company ProV&V was founded and run by Jack Cobb who formerly worked under the entity of Wyle Laboratories which is an AEROSPACE DEFENSE CONTRACTING ENTITY. The address information on the EAC, NIST and other entities for Pro V& V are different than that of what is on ProV&V website. The [EAC](#) and NIST (ISO CERT) issuers all have another address.



20. VSTLs are the most important component of the election machines as they examine the use of COTS (Commercial Off-The-Shelf)
21. “Wyle became involved with the testing of electronic voting systems in the early 1990’s and has tested over 150 separate voting systems. Wyle was the first company to obtain accreditation by the National Association of State Election Directors (NASED). Wyle is accredited by the Election Assistance Commission (EAC) as a Voting System Testing Laboratory (VSTL). Our scope of accreditation as a VSTL encompasses all aspects of the hardware and software of a voting machine. Wyle also received NVLAP accreditation to ISO/IEC 17025:2005 from NIST.” [Testimony](#) of Jack Cobb 2009
22. COTS are preferred by many because they have been tried and tested in the open market and are most economic and readily available. COTS are also the SOURCE of vulnerability therefore VSTLs are VERY important. COTS components by voting system machine manufacturers can be used as a “Black Box” and changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL) and even complete reworks to meet new standards. The key issue in this is that MOST of the COTS used by Election Machine Vendors like Dominion, ES&S, Hart Intercivic, Smartmatic and others is that such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected. This is why VSTL’s are VERY important.
23. The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates.
24. As per the COTS hardware components that are fixed, and origin may be cloaked under proprietary information a major vulnerability exists since once again third-party support software is dynamic and requires FREQUENT updates. The hardware components of the computer components, and election machines that are COTS may have slight updates that can be overlooked as they may be like those designed that support the other third -party software. COTS origin is important and the US Intelligence Community report in 2018 verifies that.
25. The Trump Administration made it clear that there is an absence of a major U.S. alternative to foreign suppliers of networking equipment. This highlights the growing dominance of

Chinese manufacturers like Huawei that are the world's LARGEST supplier of telecom and other equipment that endangers national security.

26. China, is not the only nation involved in COTS provided to election machines or the networking but so is Germany via a LAOS founded Chinese linked cloud service company that works with SCYTL named Akamai Technologies that have offices in China and are linked to the server that Dominion Software.

28 046 Madrid

Asian offices

Akamai Technologies - India

111, Brigade Court
Koramangala Industrial Area
Bangalore 560 095, India

Telephone: 91-80-575-99222
Fax: 91-80-575-99209
Regional Manager: Stuart Spiteri

Akamai Technologies - China

Suite 1560, 15th Floor
NCI Tower
12A Jianguomenwai Avenue
Chaoyang District,
Beijing 100022
China

Telephone: 86-10-8523-3097
Fax: 86-10-8523-3001
Regional Manager: Stuart Spiteri

Akamai Japan K.K.

The Executive Centre Japan K.K.
15F Tokyo Ginko Kyokai building
1-3-1 Marunouchi, Chiyoda-ku, Tokyo 100-0005

Telephone: 81-3-3216-7200 (Centre)
81-3-3216-7300 (Akamai direct)
Fax: 81-3-3216-7390 (Centre)
Regional Manager: Stuart Spiteri

Akamai Technologies - Singapore

Akamai, Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
[Driving directions](#)


Telephone: +65 6248 4614
Fax: +65 6248-4501
Regional Manager: Stuart Spiteri

Akamai Technologies - Australia and New Zealand

201 Sussex St
Tower 2, Level 20
Sydney, NSW 2000, Australia
info@au.akamai.com

Telephone: 61 2 9006 1325
Fax: 61 2 9475 0343
Regional Manager: Stuart Spiteri

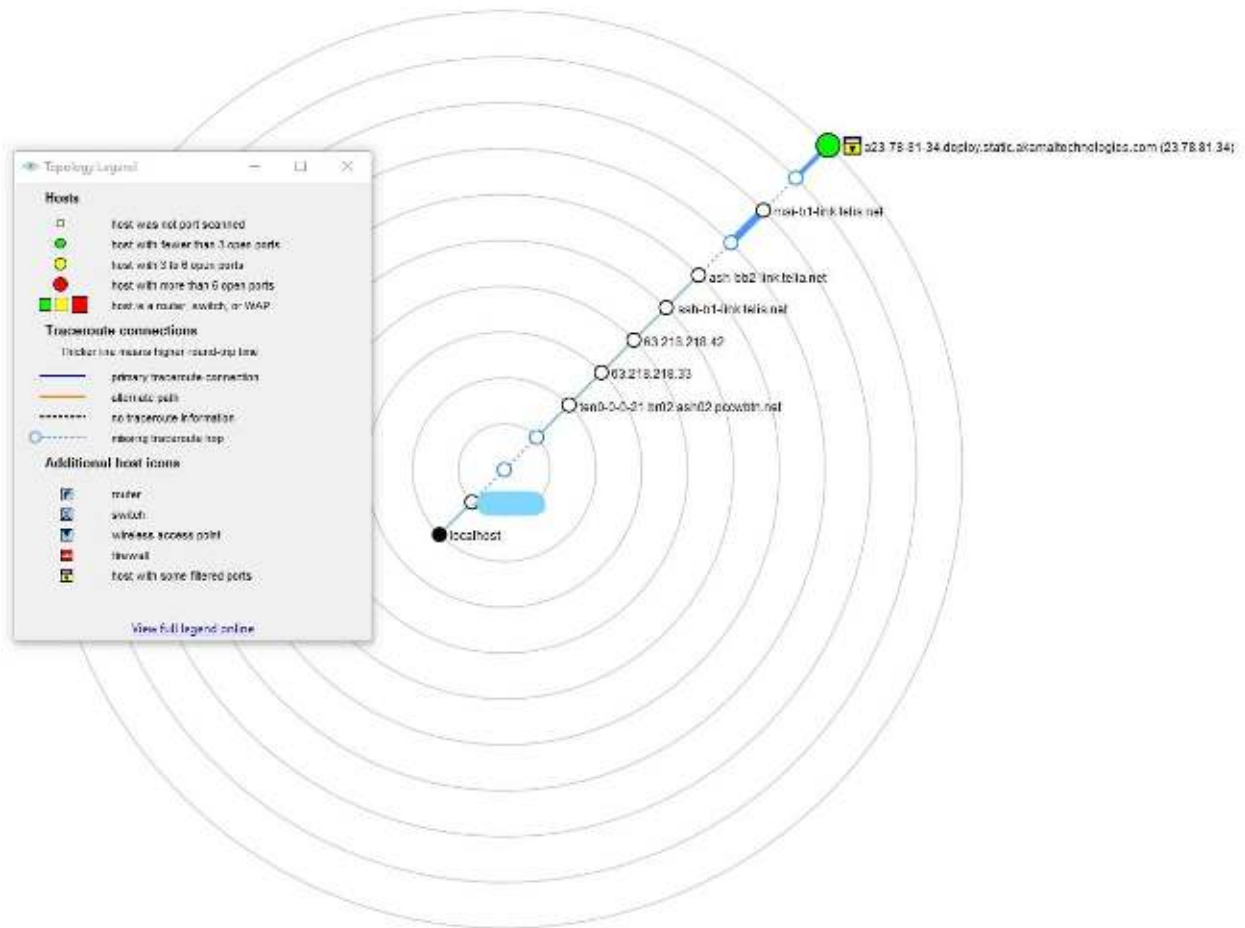
ptt.gov resolves to 4.30.228.74. According to our data this IP address belongs to Level 3 Communications and is located in Alexandria, Virginia, United States. Please have a look at the information provided below for further details.

🇺🇸 4.30.228.74	
ISP/Organization	Level 3 Communications
Location	Alexandria 22304, Virginia (VA), 🇺🇸 United States (US)
Latitude	38.8115 / 38°48'41" N
Longitude	-77.1285 / 77°7'42" W
Timezone	America/New_York
Local Time	Thu, 12 Jul 2018 19:27:40 -0400
	

27.

28. L3 Level Communications is federal contractor that is partially owned by foreign lobbyist George Soros. An article that AP ran in 2010 – spoke out about the controversy of this that has been removed. ([LINK](#)) “As for the company’s other political connections, it also appears that none other than George Soros, the billionaire funder of the country’s liberal political infrastructure, owns 11,300 shares of OSI Systems Inc., the company that owns Rapiscan. Not surprisingly, OSI’s stock has appreciated considerably over the course of the year. Soros certainly is a savvy investor.” Washington Examiner re-write.





30.

31. **L-3 Communication Systems-East** designs, develops, produces and integrates communication systems and support equipment for space, air, ground, and naval applications, including C4I systems and products; integrated Navy communication systems; integrated space communications and RF payloads; recording systems; secure communications, and information security systems. In addition, their site claims that MARCOM is an integrated communications system and The Marcom® is the foundation of the Navy's newest digital integrated voice / data switching system for affordable command and control equipment supporting communications and radio room automation. The MarCom® uses the latest **COTS** digital technology and open systems standards to offer the command and control user a low cost, user friendly, solution to the complex voice, video and data communications needs of present and future joint / allied missions. Built in reliability, rugged construction, and fail-safe circuits ensure your call and messages will go through. Evidently a HUGE vulnerability.

32. Michigan's government site is thumped off Akamai Technologies servers which are housed on **TELIA AB** a foreign server located in Germany.

33. Scytl, who is contracted with AP that receives the results tallied BY Scytl on behalf of Dominion – During the elections the AP reporting site had a disclaimer.

AP – powered by SCYTL.

Advertisements	Basic Tracking Info
	Domain: Michigan.gov [Whois Lookup - Domain Country - Domain To IP]
	IP Address: 23.78.81.34 [IP Blacklist Check]
	Reverse DNS: 34.81.78.23.in-addr.arpa
	Hostname: a23-78-81- 34.deploy.static.akamaitechnologies.com
	a12-67.akam.net >> 184.26.160.67 a11-66.akam.net >> 84.53.139.66 a1-35.akam.net >> 193.108.91.35
	Nameservers: a5-66.akam.net >> 95.100.168.66 a18-64.akam.net >> 95.101.36.64 a24-65.akam.net >> 2.16.130.65
	Location For an IP: Michigan.gov
	Continent: North America (NA)
	Country: United States  (US)
	Capital: Washington
	State: Unknown
	City Location: Unknown
	ISP: Akamai Technologies
	Organization: Akamai Technologies
	AS Number: AS1299 Telia Company AB
	something went wrong! something went wrong!
Geolocation on IP Map	Time Zone: America/North_Dakota/Center
	Local Time: 13:48:46
	Timezone GMT offset: -21600
	Sunrise / Sunset: 07:27 / 17:12
	Extra Information for an IP: Michigan.gov
	Continent Lat/Lon: 46.07305 / -100.546
	Country Lat/Lon: 38 / -98
	City Lat/Lon: (37.751) / (-97.822)
	IP Language: English

34. “Scytl was selected by the Federal Voting Assistance Program of the U.S. Department of Defense to provide a secure online ballot delivery and onscreen marking systems under a program to support overseas military and civilian voters for the 2010 election cycle and beyond. Scytl was awarded 9 of the 20 States that agreed to participate in the program (New York, Washington, Missouri, Nebraska, Kansas, New Mexico, South Carolina, Mississippi and Indiana), making it the provider with the highest number of participating States.” [PDF](#)
35. According to DOMINION : 1.4.1 Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-A consists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.
36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.
37. The purpose of VSTL’s being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures “anonymity” .
38. Algorithms within the area of this “shuffling” to maintain anonymity allows for setting values to achieve a desired goal under the guise of “encryption” in the trap-door.
39. The actual use of trapdoor commitments in Bayer-Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the “shuffling” therefore even if you deploy an algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : “[The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system](#)”
40. **Key Terms**
41. **UNIVERSAL VERIFIABILITY:** Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected) . **SCYTL FAILS UNIVERSAL VERIFIABILITY** because no mathematical proofs can determine if any votes have been manipulated.
42. **INDIVIDUAL VERIFIABILITY:** Voter cannot verify if their ballot got correctly counted. Like, if they cast a vote for ABC they want to verify it was ABC. That notion clearly discounts the need for anonymity in the first place.

43. To understand what I observed during the 2020 I will walk you through the process of one ballot cast by a voter.
44. STEP 1 |Config Data | All non e-voting data is sent to Scytel (offshore) for configuration of data. All e-voting is sent to CONFIGURATION OF DATA then back to the e-voting machine and then to the next phase called CLEANSING. **CONCERNS:** Here we see an “OR PROOF” as coined by mathematicians – an “or proof” is that votes that have been pre-tallied parked in the system and the algorithm then goes back to set the outcome it is set for and seeks to make adjustments if there is a partial pivot present causing it to fail demanding manual changes such as block allocation and narrowing of parameters or self-adjusts to ensure the predetermined outcome is achieved.
45. STEP 2|CLEANSING | The Process is when all the votes come in from the software run by Dominion and get “cleansed” and put into 2 categories: invalid votes and valid votes.
46. STEP 3|Shuffling /Mixing | This step is the most nefarious and exactly where the issues arise and carry over into the decryption phase. Simply put, the software takes all the votes, literally mixes them and then re-encrypts them. This is where if ONE had the commitment key- TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how algorithm redistributes the votes.
47. This published PAPER FROM University College London depicts how this shuffle works. In essence, when this mixing/shuffling occurs, then one doesn’t have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed.

48.

Background - ElGamal encryption

- Setup: Group \mathcal{G} of prime order q with generator g
- Public key: $pk = y = g^x$
- Encryption: $\mathcal{E}_{pk}(m; r) = (g^r, y^r m)$
- Decryption: $\mathcal{D}_x(u, v) = vu^{-x}$
- Homomorphic:

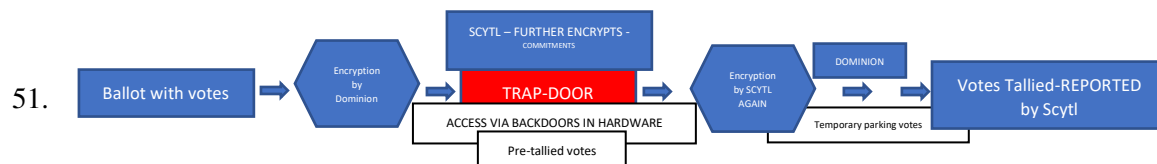
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

- Re-encryption:

$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(1; R) = \mathcal{E}_{pk}(m; r + R)$$



49. When this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes.
50. When the votes are sent to Scytl via Dominion Software EMS (Election Management System) the Trap Door is accessed by Scytl or TRAP DOOR keys (Commitment Parameters).



52. The encrypted data is shifted into Scytl's platform in the form of ciphertexts – this means it is encrypted and a key based on commitments is needed to read the data. The ballot data can only be read if the person has a key that is set on commitments.
53. A false sense of security is provided to both parties that votes are not being “REPLACED” during the mixing phase. Basically, Scytl re-encrypts the ballot data that comes in from Dominion (or any other voting software company) as ciphertexts. Scytl is supposed to prove that votes A, B, C are indeed X, Y, Z under their new re-encryption when sending back the votes that are tallied coding them respectively. This is done by Scytl and the Election Software company that agrees to certain

“Generators” and therefore together build “commitments.”

```
public CommitmentParams(final ZpSubgroup group, final int n) {
    group = group;
    h = GroupTools.getRandomElement(group);
    commitmentlength = n;
    g = GroupTools.getVectorRandomElement(group,
    this.commitmentlength);
}

// from getRandomElement(group)
Exponent randomExponent = ExponentTools.getRandomExponent(group.getQ());
return group.getGenerator().exponentiate(randomExponent);
```

54. Scytl and Dominion have an agreement – only the two would know the parameters. This means that access is able to occur through backdoors in hardware if the parameters of the commitments are known in order to alter the range of the algorithm deployed to satisfy the outcome sought in the case of algorithm failure.
55. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes. In other words, Scytl or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)

$$\text{Commitment}_{\text{CRYPT}} = \text{CM}_c$$

Saytl sets commitment - simple math ↓

$$\text{CM}_c(\vec{a}; r) = H \left(\prod_{i=1}^n G_i^{a_i} \right) = H \left(G^{\sum_{i=1}^n a_i e_i} \right)$$

$$\text{CM}_c(\vec{a}; r) \stackrel{\downarrow}{=} H \left(G^r + \sum_{i=1}^n (a_i - z_i) e_i \prod_{j=1}^n G_j^{z_j} \right) = H \left(G^r + \sum_{i=1}^n (a_i - z_i) e_i \right)$$

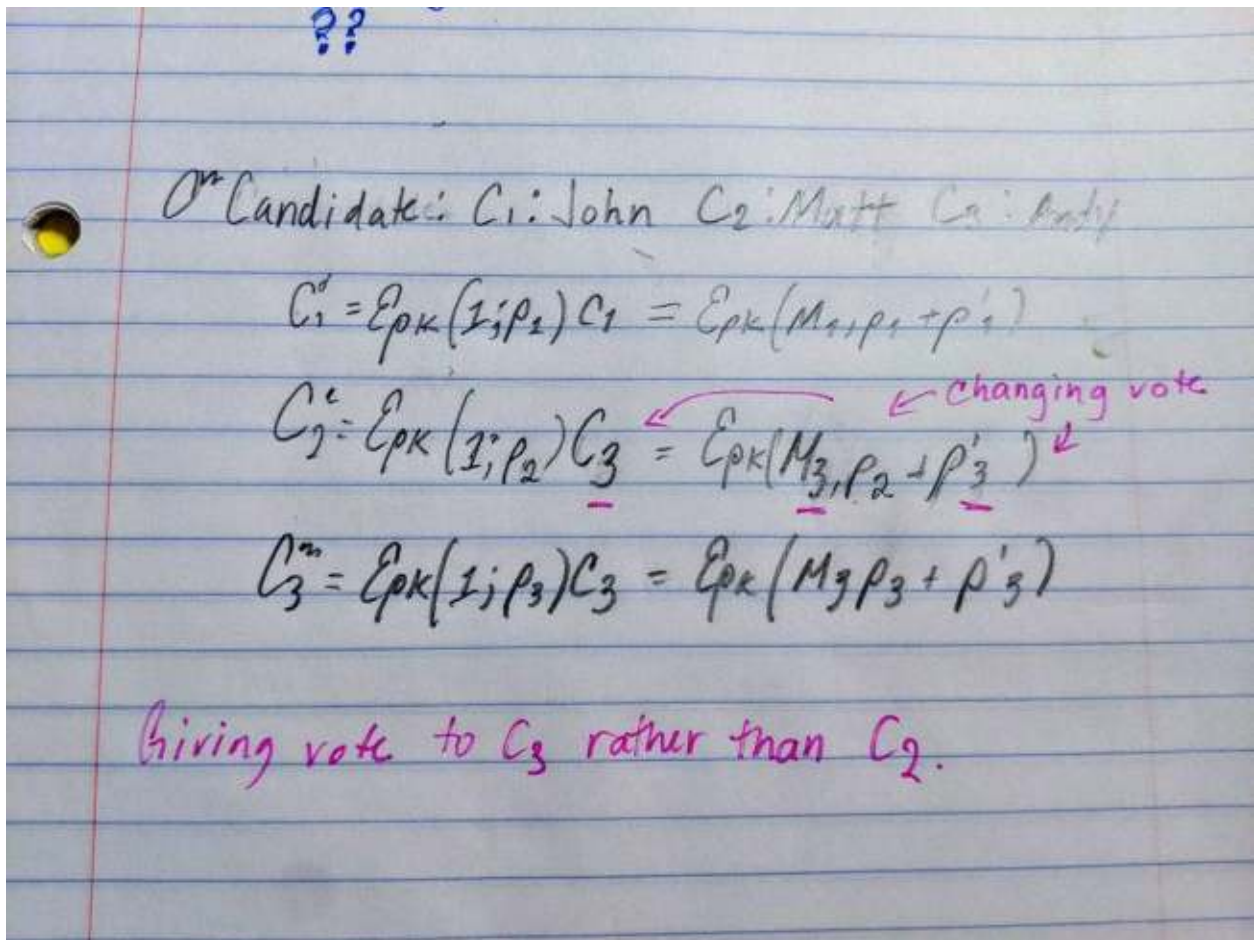
$$\text{CM}_c(\vec{a}; r) = \text{CM}_c(\vec{a}; r')$$

$$r' = r + \sum_{i=1}^n e_i (a_i - z_i)$$

56.

57. Within the trapdoor this is how the algorithm behaves to move the goal posts in elections without being detected by this proof . During the mixing phase this is the algorithm you would use to

“reallocate” votes via an algorithm to achieve the goal set.

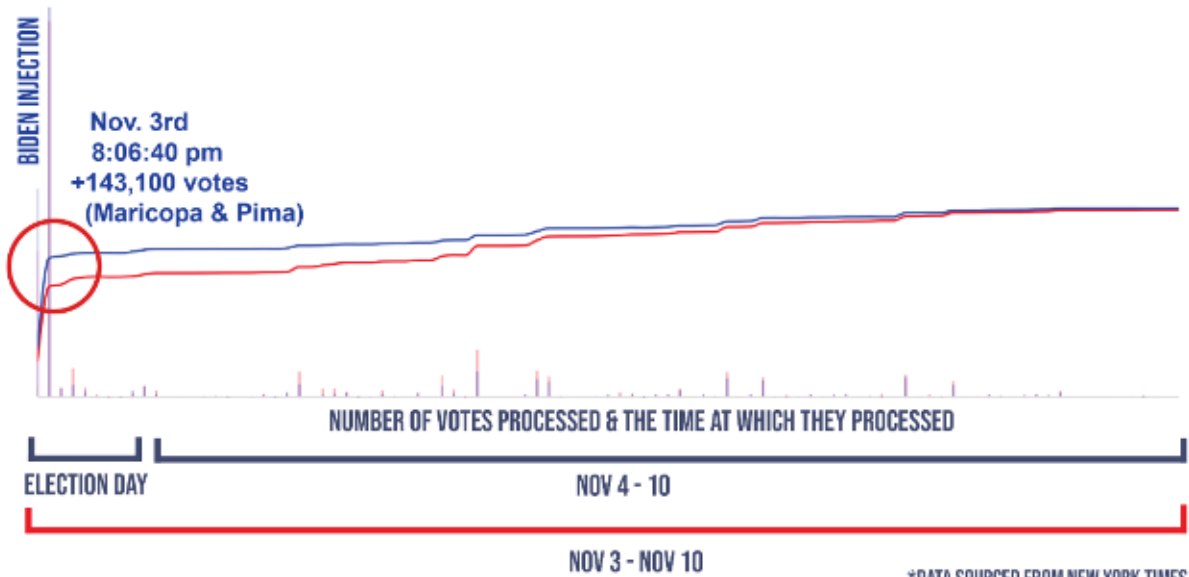


58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that the randomness is applied and used to generate the tally vote ciphertext. Thus in this case, Scytl who is the mixer can collude with their vote company clients or an agency (-----) to change votes and get away with it. This is because the receiver doesn't have the decryption key so they rely solely on Scytl to be **honest** or free from any foreign actors within their backdoor or the Election Company (like Dominion) that can have access to the key.
59. In fact, a study from the University of Bristol made claim that interference can be seen when there is a GREAT DELAY in reporting and finalizing numbers University of Bristol : [How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios](#)
60. “Zero-knowledge proofs of knowledge allow a prover to convince a verifier that she holds information satisfying some desirable properties without revealing anything else.” David Bernhard, Olivier Pereira, and Bogdan Warinschi.

61. Hence, you can't prove anyone manipulated anything. The TRAP DOOR KEY HOLDERS can offer you enough to verify to you what you need to see without revealing anything and once again indicating the inability to detect manipulation. **ZERO PROOF of INTEGRITY OF THE VOTE.**
62. Therefore, if decryption is challenged, the administrator or software company that knows the trap door key can provide you proof that would be able to pass verification (blind). This was proven to be factually true in the case study by The University of Melbourne in March. White Hat Hackers purposely altered votes by knowing the parameters set in the commitments and there was no way to prove they did it – or any way to prove they didn't.
63. IT'S THE PERFECT THREE CARD MONTY. That's just how perfect it is. They fake a proof of ciphertexts with KNOWN "RANDOMNESS". This rolls back to the integrity of the VOTE. The vote is not safe using these machines not only because of the method used for ballot "cleansing" to maintain anonymity but the EXPOSURE to foreign interference and possible domestic bad actors.
64. In many circumstances, manipulation of the algorithm is NOT possible in an undetectable fashion. This is because it is one point heavy. Observing the elections in 2020 confirm the deployment of an algorithm due to the BEHAVIOR which is indicative of an algorithm in play that had no pivoting parameters applied.
65. The behavior of the algorithm is that one point (B) is the greatest point within the allocated set. It is the greatest number within the A B points given. Point A would be the smallest. Any points outside the A B points are not necessarily factored in yet can still be applied.
66. The points outside the parameters can be utilized to a certain degree such as in block allocation.
67. The algorithm geographically changed the parameters of the algorithm to force blue votes and ostracize red.
68. Post block allocation of votes the two points of the algorithm were narrowed ensuring a BIDEN win hence the observation of NO Trump Votes and some BIDEN votes for a period of time.

ARIZONA

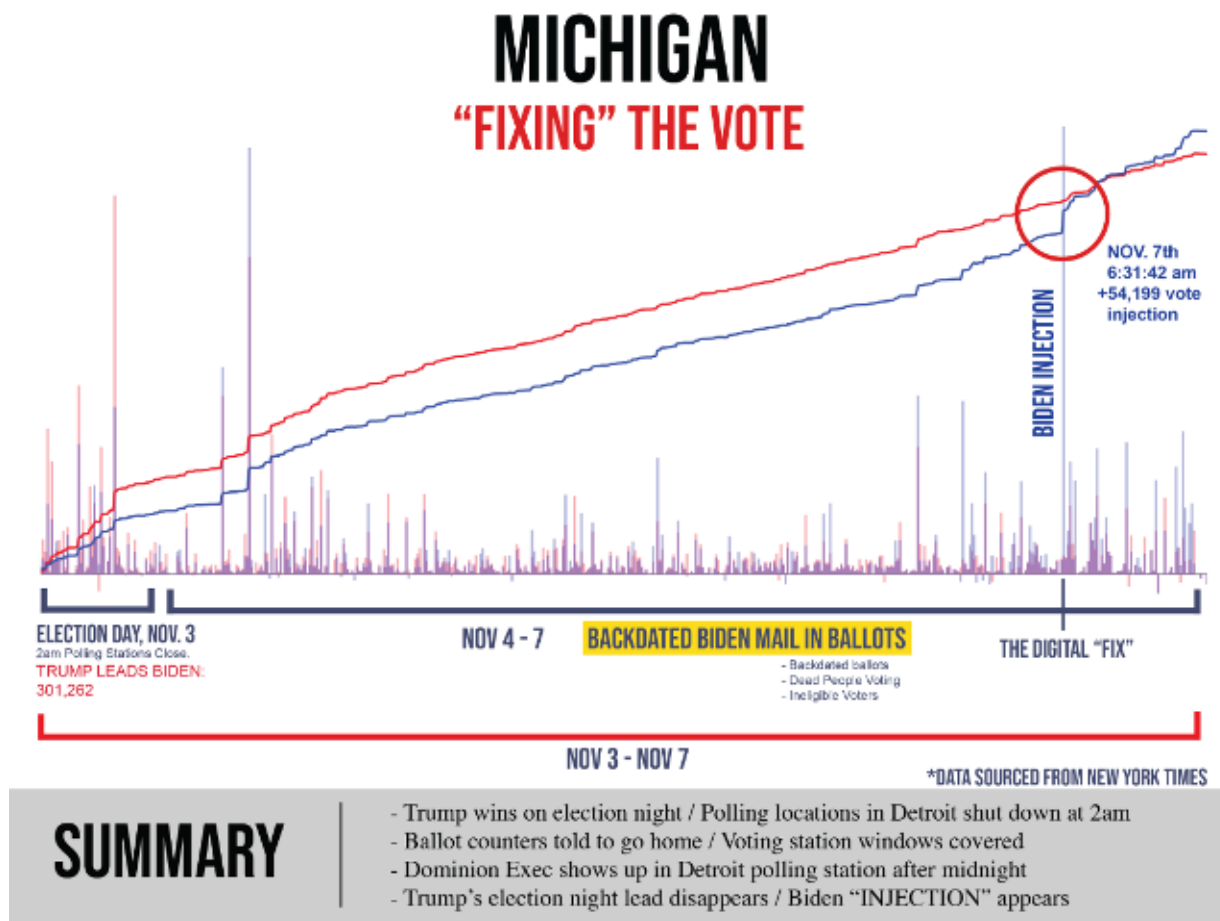
"FIXING" THE VOTE



SUMMARY

- Mathematical evidence of the seeding "injection" of votes at the beginning
- A spike means that a large number of votes were injected into the totals
- A normal vote pattern would look like a natural progression – smooth without extreme jumps

70. Gaussian Elimination without pivoting explains how the algorithm would behave and the election results and data from Michigan confirm FAILURE of algorithm.



71. The “Digital Fix” observed with an increased spike in VOTES for Joe Biden can be determined as evidence of a pivot. Normally it would be assumed that the algorithm had a Complete Pivot. Wilkinson’s demonstrated the guarantee as :

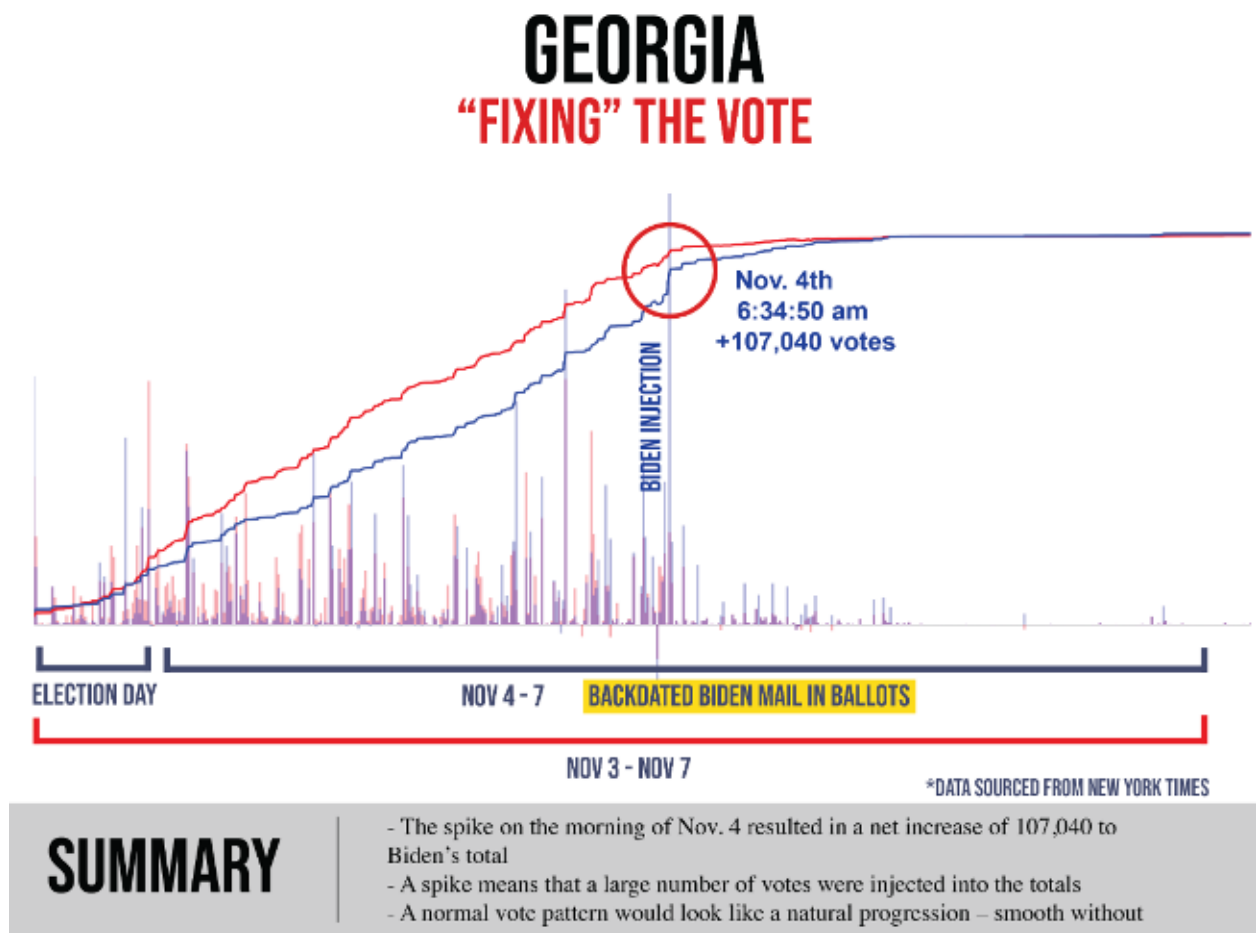
$$\frac{\|U\|_{\infty}}{\|A\|_{\infty}} \leq n^{\frac{1}{2} \log(n)}$$

72.

73. Such a conjecture allows the growth factor the ability to be upper bound by values closer to n . Therefore, complete pivoting can’t be observed because there would be too many floating points. Nor can partial as the partial pivoting would overwhelm after the “injection” of votes. Therefore, external factors were used which is evident from the “DIGITAL FIX”
74. Observing the elections, after a review of Michigan’s data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper

ballots being fed or THUMB DRIVES. The algorithm block adjusted itself and the PEOPLE were creating the evidence to BACK UP the block allocation.

75. I have witnessed the same behavior of the election software in countries outside of the United States and within the United States. In -----, the elections conducted behaved in the same manner by allocating BLOCK votes to the candidate “chosen” to win.
76. Observing the data of the contested states (and others) the algorithm deployed is identical to that which was deployed in 2012 providing Barack Hussein Obama a block allocation to win the 2012 Presidential Elections.
77. The algorithm looks to have been set to give Joe Biden a 52% win even with an initial 50K+ vote block allocation was provided initially as tallying began (as in case of Arizona too). In the am of November 4, 2020 the algorithm stopped working, therefore another “block allocation” to remedy the failure of the algorithm. This was done manually as ALL the SYSTEMS shut down NATIONWIDE to avoid detection.



- 78.
79. In Georgia during the 2016 Presidential Elections a failed attempt to deploy the scripts to block allocate votes from a centralized location where the “trap-door” key lay an attempt by someone using

84.

86. On or about April 2013 a one year plan was set to fund and usher elections in ----.

88. John Owen Brennan and James (Jim) Clapper were responsible for the ushering of the intelligence surrounding the elections in -----.

90.

The White House

Office of the Press Secretary

For Immediate Release

April 21, 2014

FACT SHEET: U.S. Crisis Support Package for Ukraine

President Obama and Vice President Biden have made U.S. support for Ukraine an urgent priority as the Ukrainian government works to establish security and stability, pursue democratic elections and constitutional reform, revive its economy, and ensure government institutions are transparent and accountable to the Ukrainian people. Ukraine embarks on this reform path in the face of severe challenges to its sovereignty and territorial integrity, which we are working to address together with Ukraine and our partners in the international community. The United States is committed to ensuring that Ukrainians alone are able to determine their country's future without intimidation or coercion from outside forces. To support Ukraine, we are today announcing a new package of assistance totaling \$50 million to help Ukraine pursue political and economic reform and strengthen the partnership between the United States and Ukraine.

SHARE THIS:

 TWITTER

 FACEBOOK

 EMAIL

91. Right before the ----- elections it was alleged that CyberBerkut a pro-Russia group infiltrated --- central election computers and **deleted key files**. These actions supposedly rendered the vote-tallying system inoperable.
92. In fact, the KEY FILES were the Commitment keys to allow Scytl to tally the votes rather than the election machines. The group had disclosed emails and other documents proving that their election was rigged and that they tried to avoid a fixed election.
93. The elections were held on May 25, 2014 but in the early AM hours the election results were BLOCKED and the final tally was DELAYED flipping the election in favor of -----.
94. The claim was that there was a DDoS attack by Russians when in actual fact it was a mitigation of the algorithm to inject block votes as we observed was done for Joe Biden because the KEYS were unable to be deployed. In the case of -----, the trap-door key was “altered”/deleted/ rendered ineffective. In the case of the US elections, representatives of Dominion/ ES&S/ Smartmatic/ Hart Intercivic would have to manually deploy them since if the entry points into the systems seemed to have failed.
95. The vote tallying of all states NATIONWIDE stalled and hung for days – as in the case of Alaska that has about 300K registered voters but was stuck at 56% reporting for almost a week.
96. This “hanging” indicates a failed deployment of the scripts to block allocate remotely from one location as observed in ----- on May 26, 2014.
97. This would justify the presence of the election machine software representatives making physical appearances in the states where the election results are currently being contested.
98. A Dominion Executive appeared at the polling center in Detroit after midnight.
99. Considering that the hardware of the machines has NOT been examined in Michigan since 2017 by Pro V& V according to Michigan’s own reporting. COTS are an avenue that hackers and bad actors seek to penetrate in order to control operations. Their software updates are the reason vulnerabilities to foreign interference in all operations exist.
100. The importance of VSTLs is underrated to protect up from foreign interference by way of open access via COTS software. Pro V& V who’s EAC certification EXPIRED on 24 FEB 2017 was contracted with the state of WISCONSIN.
101. In the United States each state is tasked to conduct and IV& V (Independent Verification and Validation) to provide assurance of the integrity of the votes.
102. If the “accredited” non-federal entities have NOT received EAC accreditation this is a failure of the states to uphold their own states standards that are federally regulated.
103. In addition, if the entities had NIST certificates they are NOT sufficing according the HAVA ACT 2002 as the role of NIST is clear.
104. Curiously, both companies PRO V&V and SLI GAMING received NIST certifications OUTSIDE the 24 month scope.

105. PRO V& V received a NIST certification on 26MAR2020 for ONE YEAR. Normally the NIST certification is good for two years to align with that of EAC certification that is good for two years.

106.



107. The last PRO V& V EAC accreditation certificate (Item 8) of this declaration expired in February 2017 which means that the IV & V conducted by Michigan claiming that they were accredited is false.
108. The significance of VSTLs being accredited and examining the HARDWARE is key. COTS software updates are the avenues of entry.
109. As per DOMINION'S own petition, the modems they use are COTS therefore failure to have an accredited VSTL examine the hardware for points of entry by their software is key.

*Compact Flash Cards	<u>***SanDisk Ultra:</u> SDCFHS-004G SDCFHS-008G <u>RiData:</u> CFC-14A RDF8G-233XMCB2-1 RDF16G-233XMCB2-1 RDF32G-233XMCB2-1 <u>SanDisk Extreme:</u> SDCFX-016G SDCFX-032G <u>SanDisk:</u> SDFAA-008G		Memory device for ICP and ICE tabulators.
*Modems	Verizon USB Modem Pantech UMW190NCD USB Modem MultiTech MT9234MU CellGo Cellular Modem E-Device 3GPUSUS AT&T USB Modem MultiTech GSM MTD-H5 Fax Modem US Robotics 56K V.92.		Analog and wireless modems for transmitting unofficial election night results.

110.

111. For example and update of Verizon USB Modem Pantech undergoes multiple software updates a year for it's hardware. That is most likely the point of entry into the systems.

112. During the 2014 elections in ---- it was the modems that gave access to the systems where the commitment keys were deleted.

113. SLI Gaming is the other VSTL "accredited" by the EAC BUT there is no record of their accreditation. In fact, SLI was NIST ISO Certified 27 days before the election which means that PA IV&V was conducted without NIST cert for SLI being valid.

United States Department of Commerce
National Institute of Standards and Technology



Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200733-0

SLI Compliance
Wheat Ridge, CO

*is accredited by the National Voluntary Laboratory Accreditation Program for specific services,
listed on the Scope of Accreditation, for:*

Voting System Testing

*This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017.
This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality
management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).*

2020-10-07 through 2020-12-31
Effective Dates



[Signature]
For the National Voluntary Laboratory Accreditation Program

- 114.
115. In fact SLI was NIST ISO Certified for less than 90 days.
116. I can personally attest that high-level officials of the Obama/Biden administration and large private contracting firms met with a software company called GEMS which is ultimately the software ALL election machines run now running under the flag of DOMINION.
117. GEMS was manifested from SOE software purchased by SCYTL developers and US Federally Funded persons to develop it.
118. The only way GEMS can be deployed across ALL machines is IF all counties across the nation are housed under the same server networks.
119. GEMS was tasked in 2009 to a contractor in Tampa, FL.
120. GEMS was also fine-tuned in Latvia, Belarus, Serbia and Spain to be localized for EU deployment as observed during the Swissport election debacle.
121. John McCain's campaign assisted in FUNDING the development of GEMS web monitoring via WEB Services with 3EDC and Dynology.

SCHEDULE B-P **ITEMIZED DISBURSEMENTS**

Use separate schedule(s)
for each category of the
Detailed Summary Page

FOR LINE NUMBER:
(check only one)

PAGE 7358 / 8595

☒ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27a
☐ 27b ☐ 28a ☐ 28b ☐ 28c ☐ 29

Any information copied from such Reports and Statements may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes, other than using the name and address of any political committee to solicit contributions from such committee.

NAME OF COMMITTEE (In Full)

JOHN MCCAIN 2008, INC.

Full Name (Last, First, Middle Initial)

A. 3EDC LLC

Mailing Address 211 NORTH UNION ST STE 200

City ALEXANDRIA State VA Zip Code 22314

Purpose of Disbursement
WEB SERVICE

Candidate Name

Category/
Type

Office Sought:

☐ House
☐ Senate
☐ President

Disbursement For: 2008

☒ Primary ☐ General
☐ Other (specify) ▼

State:

District:

Date of Disbursement

MM / DD / YYYY
03 / 17 / 2008

Transaction ID : SB23.10515

Amount of Each Disbursement this Period

399916.09

Full Name (Last, First, Middle Initial)

B. A FARE EXTRAORDINAIRE

Mailing Address 2035 MARSHALL

City HOUSTON State TX Zip Code 77098

Purpose of Disbursement
FACILITY RENTAL/CATERING

Candidate Name

Category/
Type

Office Sought:

☐ House
☐ Senate
☐ President

Disbursement For: 2008

☒ Primary ☐ General
☐ Other (specify) ▼

State:

District:

Date of Disbursement

MM / DD / YYYY
03 / 17 / 2008

Transaction ID : SB23.10049

Amount of Each Disbursement this Period

23697.69

Full Name (Last, First, Middle Initial)

C. ADMINISTAFF

Mailing Address PO BOX 203332

City HOUSTON State TX Zip Code 77216

Purpose of Disbursement
INSURANCE

Candidate Name

Category/
Type

Office Sought:

☐ House
☐ Senate
☐ President

Disbursement For: 2008

☒ Primary ☐ General
☐ Other (specify) ▼

State:

District:

Date of Disbursement

MM / DD / YYYY
03 / 05 / 2008

Transaction ID : SB23.10117

Amount of Each Disbursement this Period

483.68

Subtotal Of Receipts This Page (optional).....

424097.46

Total This Period (last page this line number only).....

122.

123.

124. AKAMAI Technologies services SCYTL.

125. AKAMAI Technologies Houses ALL foreign government sites. (Please see White Paper by Akamai.)
126. AKAMAI Technologies houses ALL .gov state sites. (ref Item 123 Wisconsin.gov Example)



- 127.
128. Wisconsin has EDGE GATEWAY port which is AKAMAI TECHNOLOGIES based out of GERMANY.
129. Using AKAMAI Technologies is allowing .gov sites to obfuscate and mask their systems by way of HURRICANE ELECTRIC (he.net) Kicking it to anonymous (AKAMAI Technologies) offshore servers.

Hosts	General	Services	Traceroute
wisconsin.gov (165.189.150.147)			
	3	3.00	207.89.33.137
	4	4.00	10.40.50.7
	5	13.00	172.22.7.24
	6	15.00	206.126.236.37 10gigabitethernet2-2.core1.ash1.he.net
	7	41.00	184.105.64.133 100ge1-1.core2.chi1.he.net
	8	27.00	184.104.192.117 100ge15-2.core1.chi1.he.net
	9	32.00	184.105.65.226 100ge8-1.core1.msn1.he.net
	10	35.00	216.66.73.242 airstream-communications-llc.10gigabitethernet2-20.core1.msn1.he.net
	11	37.00	64.33.130.57 air-cpdg-asr-to-mdsn.airstreamcomm.net.130.33.64.in-addr.arpa
	12	37.00	64.33.143.186 win-retail-wi-doa-001-2.direct.airstreamcomm.net
	13		<unknown>
	14		<unknown>
	15	38.00	165.189.150.147

- 130.
131. AKAMAI Technologies has locations around the world.
132. AKAMAI Technologies has locations in China (ref item 22)
133. AKAMAI Technologies has locations in Iran as of 2019.
134. AKAMAI Technologies merged with UNICOM (CHINESE TELECOMM) in 2018.
135. AKAMAI Technologies house all state .gov information in GERMANY via TELIA AB.

136. In my professional opinion, this affidavit presents unambiguous evidence:
137. That there was Foreign interference, complicit behavior by the previous administrations from 1999 up until today to hinder the voice of the people and US persons knowingly and willingly colluding with foreign powers to steer our 2020 elections that can be named in a classified setting.
138. Foreign interference is present in the 2020 election in various means namely,
139. Foreign nationals assisted in the creation of GEMS (Dominion Software Foundation)
140. Akamai Technologies merged with a Chinese company that makes the COTS components of the election machines providing access to our electronic voting machines.
141. Foreign investments and interests in the creation of the GEMS software.
142. US persons holding an office and private individuals knowingly and willingly oversaw fail safes to secure our elections.
143. The EAC failed to abide by standards set in HAVA ACT 2002.
144. The IG of the EAC failed to address complaints since their appointment regarding vote integrity
145. Christy McCormick of the EAC failed to ensure that EAC conducted their duties as set forth by HAVA ACT 2002
146. Both Patricia Layfield (IG of EAC) and Christy McCormick (Chairwoman of EAC) were appointed by Barack Hussein Obama and have maintained their positions since then.
147. The EAC failed to have a quorum for over a calendar year leading to the inability to meet the standards of the EAC.
148. AKAMAI Technologies and Hurricane Electric raise serious concerns for NATSEC due to their ties with foreign hostile nations.
149. For all the reasons above a complete failure of duty to provide safe and just elections are observed.
150. For the people of the United States to have confidence in their elections our cybersecurity standards should not be in the hands of foreign nations.
151. Those responsible within the Intelligence Community directly and indirectly by way of procurement of services should be held accountable for assisting in the development, implementation and promotion of GEMS.
152. GEMS ----- General Hayden.
153. In my opinion and from the data and events I have observed ----- with the assistance of SHADOWNET under the guise of L3-Communications which is MPRI. This is also confirmed by [us.army.mil](https://www.us.army.mil) making the statement that shadownet has been deployed to 30 states which all

happen to be using Dominion Machines.

FAIRFAX, Va. -The Virginia National Guard's Bowling Green-based 91st Cyber Brigade completed the nationwide rollout of its ShadowNet enterprise solution July 19, 2019, with the integration of the 125th Cyber Protection Battalion into the solution's virtual private network. ShadowNet is a custom-built private cloud-based out of the brigade's data center in Fairfax, Virginia, that uses VPN connectivity to provide its aligned units with 24-hour, seven-days-a-week remote access to critical cyber training at both the collective and individual levels. The brigade successfully integrated its three other cyber protection battalions - the 123rd, 124th, and 126th Cyber Protection Battalions - into the ShadowNet platform last January.

"I'm extremely proud to announce that the Soldiers of the 91st Cyber Brigade have completed the construction and rollout of ShadowNet, a world-class enterprise solution designed to propel operational innovation in the field of cyber training," said Col. Adam C. Volant, commander of the 91st Cyber Brigade. "ShadowNet will allow us to leverage the expertise of cyber professionals across our four cyber protection battalions to build Soldier-centric programs and collective training environments that deliver

OCTOBER 26, 2020

U.S. Army STAND-TO! | Army Readiness Training

SEPTEMBER 12, 2019

September 2017 Nominative Sergeant Major Assignments

SEPTEMBER 12, 2019

DA ANNOUNCES ROTATIONAL DEPLOYMENTS

154. Based on my research of voter data – it appears that there are approximately 23,000 residents of a Department of Corrections Prison with requests for absentee ballot in Wisconsin. We are currently reviewing and verifying the data and will supplement.

	23230	Gutierrez	Mary	Jane		(262)994-9050	
23231	23231	Hansen	Luann	M		(262)994-9050	
23232	23232	Neberman	John	C		(262)994-9050	
23233	23233	Reynolds	Devi	J		(262)994-9050	
23234	23234	Rieckhoff	Kathryn	Susan		(262)994-9050	
23235	23235	Edwards	Mark	Landon		(262)994-9050	
23236	23236	Pfeiffer	Joseph	Patrick		(262)994-9050	
23237	23237	Hines	Dianna	K		(262)994-9050	
23238	23238	Beachem	Janice	F		(262)994-9050	
23239	23239	Blackstone	Thomas	Wayne		(262)994-9050	
23240	23240	Braun	Patricia	Ann		(262)994-9050	
23241	23241	Smith	Raymond	L		(262)994-9050	
23242	23242	Meyer	Steven	R		(262)994-9050	
23243	23243	Vincent	Herbert			(262)994-9050	
23244	23244	Guajardo	Juan	P		(262)994-9050	
23245	23245	Wallace	Kirk	R		(262)994-9050	
23246	23246	Kaplan	Bernard	L		(262)994-9050	
23247	23247	Bahrs	Michelle	M		(262)994-9050	
23248	23248	Shattuck	Elizabeth	L		(262)994-9050	
23249	23249	Munoz	Rosalio	S	JR	(262)994-9050	
23250	23250	Strunk	Amy	C		(262)994-9050	
23251	23251	Schendel	Michael	P	JR	(262)994-9050	
23252	23252	Mack	Kimberly	N		(262)994-9050	
23253	23253	Spikes	Debra	A		(262)994-9050	
23254	23254	Busarow	Suzanne	M		(262)994-9050	
23255	23255	Oliver	Timmy			(262)994-9050	
23256	23256	Wember	Jimmy	Dean		(262)994-9050	
23257	23257	Kosterman	Michael	Richard		(262)994-9050	
23258	23258	Szaradowski	Paul	M		(262)994-9050	
23259	23259	Oliver	Dale			(262)994-9050	
23260	23260	Derango	Nancy			(262)994-9050	
23261	23261	Smith	Arthur	J		(262)994-9050	SMITH24.3059@YAHOO
23262	23262	Brown	Michael	Edward		(262)994-9050	

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge.

Executed this November 29th, 2020.

A handwritten signature in black ink, appearing to read 'Terpsehore P Maras', with a stylized, cursive script.

Terpsehore P Maras

From: [Adriel Lam](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Oral Testimony for Sep 16 Elections Commission meeting
Date: Friday, September 16, 2022 9:44:52 AM
Attachments: [ORAL TESTIMONY FOR ELECTIONS COMMISSION MEETINGS.pdf](#)
[unclearballot.pdf](#)
[Same 29JUN ListID different 22JUL ballot name v2.png](#)

Aloha, I would like to present Oral Testimony for today's Elections Commission meeting at 10am.

Aloha,
Adriel Lam

ORAL TESTIMONY FOR ELECTIONS COMMISSION MEETINGS, SEPTEMBER 16, 2022

Aloha Chair Anderson, Commissioners and Chief Elections Officer Nago,

The public was told in 2019 that Elections by Mail would increase voter participation and reduce the cost of our elections. I would ask the Commission to review the facts and reconsider this overreliance on electronic voting systems and Elections by Mail.

2022 Kauai Special Election 25.74% participation

2022 Primary Election 39.8% participation

2018 Precinct Elections Actual Expense \$6,477,477 (revised from \$7,391,411)

2020 Election By Mail Actual Expense \$8,471,522 (projected \$6,420,531)

2022 Elections By Mail Projected Expense \$8,204,760

Voter participation has not improved and neither has Elections By Mail gotten any more cost effective.

Voter confidence in the conduct of our elections continue to erode, when known vulnerabilities and errors are public knowledge, yet HRS 16-42 is not being followed to alleviate these concerns:

At the DEFCON 21 cybersecurity conference, University of Michigan graduate student presented Unclear Ballot: Automated Ballot Image Manipulation - DEF CON 27 Voting Village.

<https://www.youtube.com/watch?v=ja6J1wY2UNw>

- Post-election audits must inspect paper ballots.
- Actual attack has no visual components.
- Tested on Hart Verity with 181,541 ballots from Nov 6, 2016 Clackamas County.
- Altered 62,400 (34%), alteration time 279 milliseconds, Hart scan time 352 milliseconds.
- No vendor has minimal image detection in software.

Attached: Unclear Ballot, Automated Ballot Image Manipulation (18 page)

In the 2022 Georgia DeKalb County Commissioner Democratic Primary, third-place finisher Michelle Long Spears was declared the first-place finisher after hand recount of the ballots. The original first-place finisher Marshall Orson ended up in third place.

At the April 1 Election Commission meeting, Chair Anderson asked that in lieu of an investigation a that a security report would be provided to the Commissioners.

In Kauai County, ballots were presented to the Counting Center pre-sorted by precincts. Ballots were then mixed by the Counting Center into unsorted batches for scanning and tallying.

To date, no known physical tallies of any precinct has been done to come close to satisfying requirements of HRS 16-42(b)(3) "that the electronic tallies generated by the system in those precincts equal hand tallies of the paper ballots generated by the system in those precincts;" such that electronic voting systems can be relied upon "in lieu of counting the paper ballots by hand or with a mechanical tabulation system" as provided under HRS 16-42(b)(1).

Hand counting of paper ballots isn't a time-consuming or complex process. It is a tried and true method that technologically advanced countries and economies like Taiwan and France have relied upon to conduct their elections. A 13-14 person team, assigned to precincts of 1500-1700 voters can accomplish this task in less than six hours. Elections and politics are a people process, not machines, this puts elections back in the hands of the people.

Sincerely,

Adriel Lam
Vice Chair, Election Integrity
Hawaii Republican Party

ListID	vrNameLast	vrNameFirst	noResAddress	LastName	FirstName	ResidenceAddress
DB4E57D1AA0C4567860A8E9018157709	CALVIN	JAY	2140 KUHIO AVE	LU	CALVIN	2140 KUHIO AVE
D6D92FFD132A48B9833BFD27D221A014	DACANAY	DAVID	98-358 PONOKIWILA ST	TAKENAKA	MAYUKO	909 COOLIDGE ST
29247D49DC4E4F7DB968FBD6E2B1D576	HAWAII	UNITED	46-395 KAHUHIPA ST	KAHOOHANO HANO	EDMUND	46-395 KAHUHIPA ST
6D5618B65B1C4ADDB9DC47CB3ACC2428	KENNETH	CARTER	565 PAPALANI ST	CARTER	KENNETH	45-623 HINAMOE LOOP
C7C7023C2B1C4E0F8F567F2C41F32398	LOCHAN	VISHNU	2464 PRINCE EDWARD ST	JAMES	JOHN	2464 PRINCE EDWARD ST
F1BFB1EF565645ECA57D4E5C86946D4E	PANTE	KELLY	94-447 KAHUALOA PL	PENALES	KELLY CRISTLE	94-447 KAHUALOA PL
901F923B7B2348688CBF4E1B375F443F	PINOLIAD	LUCCI	99-180 KULINA ST	FONTANILLA	EUGENIO	99-304 EKE PL
F6D6668802BB43409650F16E082DD92D	RODNEY	MORIYAMA	1305 MOANALUALANI PL	MORIYAMA	RODNEY	1305 MOANALUALANI PL
BBB9A7A049134C4AA9460C5D5AFF43E4	WILLIAMS	DAWN	47-665 WAILEHUA PL	SHARPE	DIANA	94-668 KUPUNA LOOP
D85AD40BE1E9481AB0A52E991405F0D8	YOUNG	JAMIE	2510 KEKUANONI ST	TOM	JAMIE ANNE	2937 LOWREY AVE

UnclearBallot: Automated Ballot Image Manipulation

Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman

Department of Electrical Engineering and Computer Science, University of Michigan
{matber, kartkand, jreremy, jhalderm}@umich.edu

Abstract. As paper ballots and post-election audits gain increased adoption in the United States, election technology vendors are offering products that allow jurisdictions to review ballot images—digital scans produced by optical-scan voting machines—in their post-election audit procedures. Jurisdictions including the state of Maryland rely on such image audits as an alternative to inspecting the physical paper ballots. We show that image audits can be reliably defeated by an attacker who can run malicious code on the voting machines or election management system. Using computer vision techniques, we develop an algorithm that automatically and seamlessly manipulates ballot images, moving voters’ marks so that they appear to be votes for the attacker’s preferred candidate. Our implementation is compatible with many widely used ballot styles, and we show that it is effective using a large corpus of ballot images from a real election. We also show that the attack can be delivered in the form of a malicious Windows scanner driver, which we test with a scanner that has been certified for use in vote tabulation by the U.S. Election Assistance Commission. These results demonstrate that post-election audits must inspect physical ballots, not merely ballot images, if they are to strongly defend against computer-based attacks on widely used voting systems.

Keywords: optical scan, paper ballots, image manipulation, drivers, image processing

1 Introduction

Elections that cannot provide sufficient evidence of their results may fail to adequately gain public confidence in their outcomes. Numerous solutions have been posited to this problem [9], but none has been as elegant, efficient, and immediately practical as post-election audits [21, 25, 39]. These audits—in particular, ones that seek to limit the risk of confirming an outcome that resulted from undue manipulation—are one of the most important layers of defense for election security [32].

Risk-limiting audits (RLAs) rely on sampling robust, independent evidence trails created by voter-verified paper ballots. However, other types of post-election

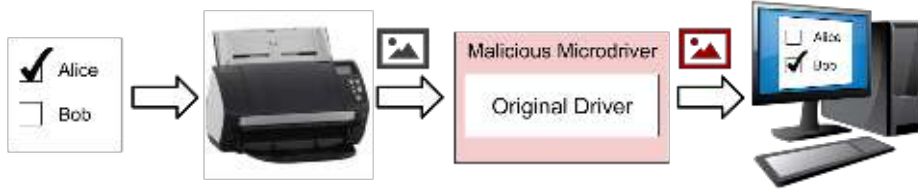


Fig. 1. Attack overview—A voter’s paper ballot is scanned by a ballot tabulator, producing a digital image. Malware in the tabulator—in our proof-of-concept, a microdriver that wraps the scanner device driver—alters the ballot image before it is counted or stored. A digital audit shows only the manipulated image.

audits are gaining popularity in the marketplace. In particular, Clear Ballot, an election technology vendor in the United States, pioneered audit software designed to perform audits of *images* of ballots which have been scanned and tabulated, which we shall refer to as “image audits”. Other vendors have adopted support for this kind of audit, and one U.S. state, Maryland, relies on image audits to provide assurances of its election results [33].

While image audits can help detect human error and aid in adjudicating mismarked ballots, we show that they cannot provide the same level of security assurance as audits of physical ballots. Since ballot images are disconnected from the actual source of truth—physical paper ballots—they do not necessarily provide reliable evidence of the outcome of an election under adversarial conditions.

In this paper, we present UnclearBallot, an attack that defeats image audits by automatically manipulating ballot images as they are scanned. Our attack leverages the same computer vision approaches used by ballot scanners to detect voter selections, but adds the ability to move marks from one target area to another. Our method is robust to inconsistent or invalid marks, and can be adapted to many ballot styles.

We validate our attack against a corpus of over 180,000 ballot images from the 2018 election in Clackamas County, Oregon, and find that UnclearBallot can move marks on 34% of the ballots while leaving no visible anomalies. We also test our attack’s flexibility using six widely used styles of paper ballots, and its robustness to invalid votes using an established taxonomy of voter marks. As a proof-of-concept, we implement the attack in the form of a malicious Windows scanner driver, which we test using a commercial-off-the-shelf scanner certified for use in elections by the U.S. Election Assistance Commission.

UnclearBallot illustrates that post-election audits in traditional voting systems must involve rigorous examination of *physical ballots*, rather than ballot images, if they are to provide a strong security guarantee. Without an examination of the physical evidence, it will be difficult if not impossible to assure that computer-based tampering has not occurred.

The remainder of this paper is organized as follows: Section 2 provides background on image audits, ballot scanners, and image processing techniques we use to implement our attack. Section 3 describes the attack scenarios against

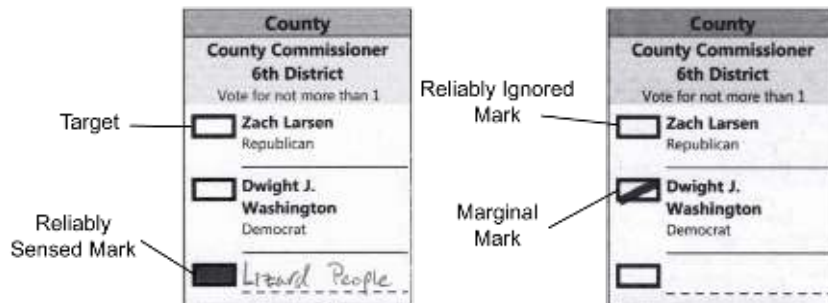


Fig. 2. Terms for parts of a marked ballot, following Jones [23].

optical scanners and image audits. Section 4 explains the methodology of our attack. In Section 5 we present data indicating that our attack can be robust to various ballot styles and voter marks. Section 6 contextualizes our attacks and discusses mitigations. We conclude in Section 7.

2 Background

Our attack takes advantage of two aspects of optical scanner image audits: the scanning and image processing techniques used by scanners, and the reliance on scanned images by image audits. Here we provide a brief discussion of both.

2.1 Ballot Images

Jones [23] put forth an analysis of the way that ballot scanners work, particularly the mark-sense variety that is most common today. All optical scanners currently sold to jurisdictions, as well as the vast majority of scanners used in practice in the U.S., rely on mark-sense technology [44]. Scanners first create a high-resolution image of a ballot as it is fed past a scan head. Software then analyzes the image to identify dark areas where marks have been made by the voter.¹ Once marks have been detected, systems may use template matching to translate marks into votes for specific candidates, typically relying on a barcode or other identifier on the ballot that specifies a ballot style to match to the scanned image.

Detecting and interpreting voter marks can be a difficult process, as voters exhibit a wide range of marking and non-marking behavior, including not filling in targets all the way, resting their pens inside targets, or marking outside the target. The terms Jones developed to refer to the ballot and marks are illustrated in Figure 2. Marks that adequately fill the target and are unambiguously interpreted as votes by the scanner are called *reliably sensed* marks, and targets that are unambiguously not filled and therefore not counted are *reliably ignored* marks.

¹ The details of how marks are identified vary by hardware and scanning algorithm. See [13] for an example.

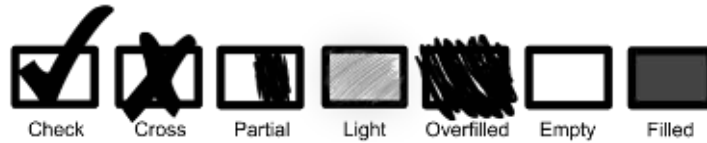


Fig. 3. Taxonomy of voter marks adapted from Bajcsy [2], including the five leftmost marks that may be considered marginal marks.

Marks of other types are deemed *marginal*, as a scanner may read or ignore them. Moreover, whether a mark should be counted as a vote is frequently governed by local election statute, so some marginal marks may be unambiguously counted or ignored under the law, even if not by the scanner.

Bajcsy et al. [2] further develops a systematization of marginal marks and develops some improvements on mark-detection algorithms to better account for them. An illustration of Bajcsy et al.’s taxonomy is shown in Figure 3. Ji et al. [22] discuss different types of voter marks as applied to write-in votes, as well as developing an automated process for detecting and tabulating write-in selections.

2.2 Image Audits

Risk-limiting post-election audits rely on physical examination of a statistical sample of voter-marked ballots [24, 26, 39, 40]. However, this can create logistical challenges for election officials, which has prompted some to propose relaxations to traditional audit requirements. To reduce workload, canvass audits and recounts in many states rely on retabulation of ballots through optical scanners (see the 2016 Wisconsin recount, for example [31]).

Some election vendors take retabulation audits a step further: rather than physically rescan the ballots, the voting system makes available images of all the ballots for independent evaluation after the election [15, 16, 42].² While the exact properties of these kinds of image audits vary by vendor, they typically rely on automatically retabulating all or some images of cast ballots, as well as electronic adjudication for ballots with marginal marks. These “audits” never examine the physical paper trail of ballots, which our attack exploits.

Several jurisdictions have relied on these image audits, including Cambridge, Ontario, which used Dominion’s AuditMark [17], and the U.S. state of Maryland, which uses Clear Ballot’s ClearAudit [28]. Maryland has also codified image audits into its election code, requiring that an image audit be performed after every election [27].

² While the review is made available to the public, the actual images themselves are seldom published in full out of concern for voter anonymity.

3 Attack Scenarios

Elections in which voters make their selections on a physical ballot are frequently held as the gold standard for conducting a secure election [32]. However, the property that contributes most to their security, software independence [34], only exists if records computed by software are checked against records that cannot be altered by software without detection. Image audits enable election officials to view images of ballots and compare them with the election systems’ representation of the particular ballot they are viewing (called a cast vote record or CVR). While these two trails of evidence may be independent from each other (for example, Clear Ballot’s ClearAudit [15] technology can be used to audit a tabulation performed by a different election system altogether), they are not software independent. A clever attacker can exploit the reliance on software by both evidence trails to defeat detection.

To surreptitiously change the outcome of the election in the presence of an image audit, the attacker must alter both the tabulation result as well as the ballot images themselves. Researchers have documented numerous vulnerabilities that would allow an attacker to infect voting equipment and change tabulation results (see [10, 20, 30] among others), so we focus on the feasibility of manipulating ballot images once an attacker has successfully infected a machine where they are stored or processed.

The most straightforward attack scenario occurs when the ballot images are created by the same equipment that produces the CVR. In this case, the attacker can simply infect the scanner or tabulator with malware that corrupts both the CVR and the images at the same time. The attack could change the image before the tabulator processes it to generate the CVR, or directly alter both sets of records.

In some jurisdictions, the ballot images that are audited are collected in a separate process from tabulation—that is, by scanning the ballots again, as in Maryland’s use of ClearAudit from 2016 [28]. In this case, the adversary has to separately attack both processes, and has to coordinate the cheating to avoid mismatches between the initial tally and the altered ballot images.

Depending on the timing of the audit, manipulation of ballot images need not be done on the fly. For example, if the ballot images are created during tabulation but the image audit does not occur until well after the election, an attacker could modify the ballot images while they are in storage.

For ease of explication, the discussion that follows assumes that ballot images are created at the time of tabulation, in a single scan. The attack we develop targets a tabulation machine and manipulates each ballot online as it is scanned.

4 Methodology

To automatically modify ballot images, an attacker can take a few approaches. One approach would be to completely replace the ballot images with ballots filled in by the attacker. However, this risks being detected if many ballots have

the same handwriting, and requires sneaking these relatively large data files into the election system without being detected. For these reasons, we investigate an alternative approach: automatically and selectively doctoring the ballot scans to change the vote selections they depict.

For the attack to work successfully, we need to move voter marks to other targets without creating visible artifacts or inconsistencies. We must be able to dynamically detect target areas and marks, alter marks in a way that is consistent with the voter’s other marks, and do so in a way that is undetectable to the human eye. However, there is a key insight that works in the adversary’s favor: an attacker seeking to alter election results does not have to be able to change *all* ballots undetectably, only sufficiently many to swing the result. This means that the attacker’s manipulation strategy is not required to be able to change *every* mark—it merely has to reliably detect *which* marks it can safely alter and change enough of them to decide the election result.

4.1 Reading the ballot

To interpret ballot information, we rely on the same techniques that ballot scanners use to convert paper ballots into digital representations. Attackers have access to the ballot templates, as jurisdictions publish sample ballots well ahead of scheduled elections. Using template matching, an attacker does not have to perform any kind of sophisticated character recognition, they simply have to find target areas and then detect which of the targets are filled.

Our procedure to read a ballot is illustrated in Figure 4. First, we perform template matching to extract each individual race within a ballot. Next, we use OpenCV’s [11] implementation of the Hough transform to detect straight lines that separate candidates and break the race into individual panes for each candidate. Notably, the first candidate in each race may have the race title and extra information in it (see Figure 4c), which is cropped out based on white space.

Target areas are typically printed on the ballot as either ovals or rectangles. To detect them, we construct a bounding box around the target by scanning horizontally from the left of the race and then vertically from the bottom up, and compute pixel density values. The bounds are set to the coordinates where the density values first increase and last decrease. Once we have detected all the target areas, we compute the average pixel density of the area within the bounding box to determine whether or not a target area is marked. We then use our template to convert marks into votes for candidates.

4.2 Changing marks

Once we have identified which candidate was marked by the voter, we can move the mark to one of the other target locations we identified. If the vote is for a candidate the attacker would like to receive fewer votes—or if it is not a vote for a candidate they would like to win—the attacker can simply swap the pixels within the bounding boxes of the voter’s marked candidate and an unmarked candidate.

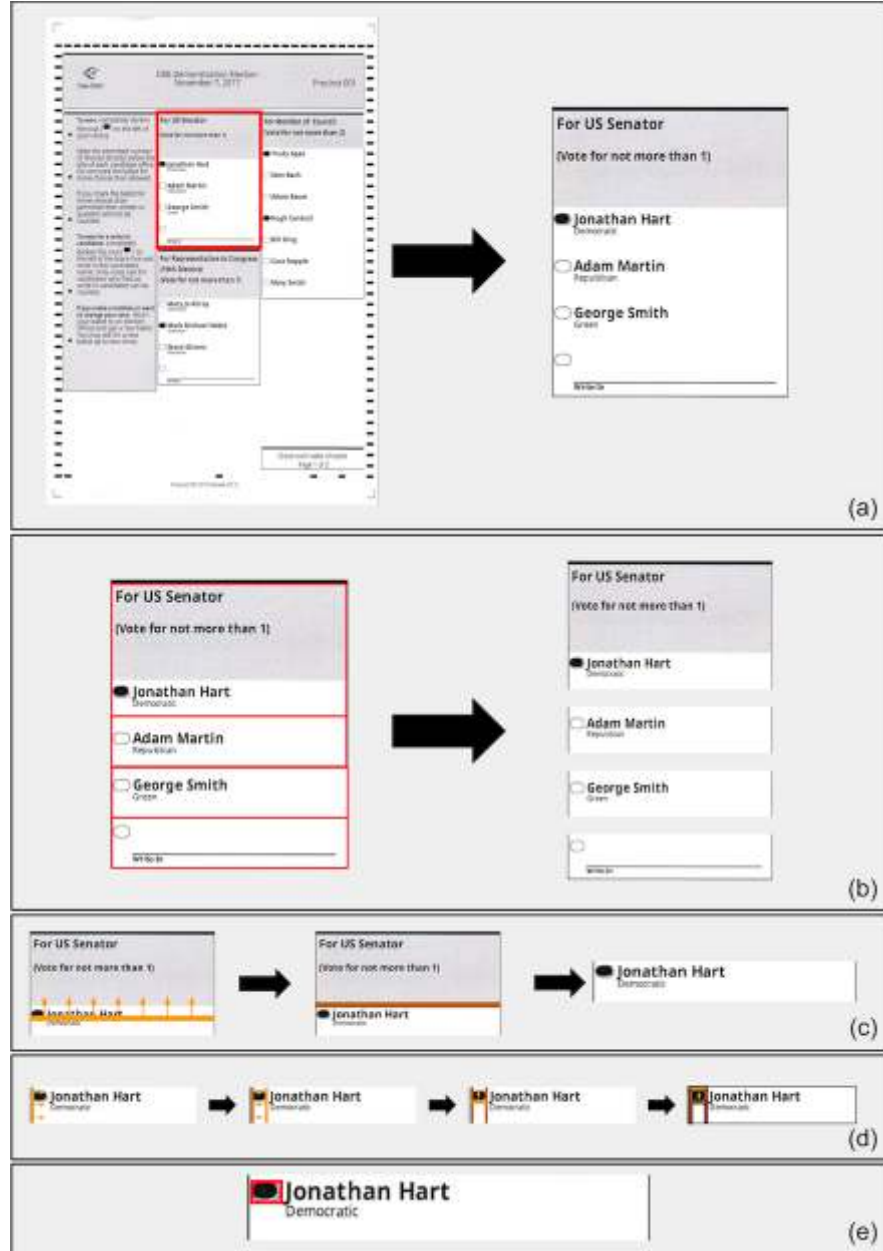


Fig. 4. Ballot manipulation algorithm—First, (a) we apply template matching to extract the race we intend to alter. Then, (b) we use Hough line transforms to separate each candidate. If the first candidate has a race title box, (c) we remove it by computing the pixel intensity differences across a straight line swept vertically from the bottom. For each candidate, (d) we identify the target and mark (if present) by doing four linear sweeps and taking pixel intensity. Finally, (e) we identify and move the mark. At each step we apply tests to detect and skip ballots where the algorithm might leave artifacts.

Original		Manipulated	
County		County	
Supervisor, District 1		Supervisor, District 1	
	Vote for One		Vote for One
Alfred Hitchcock	<input checked="" type="radio"/>	Alfred Hitchcock	<input type="radio"/>
Vincent Price	<input type="radio"/>	Vincent Price	<input checked="" type="radio"/>
Write In	<input type="radio"/>	Write In	<input type="radio"/>
State		State	
Governor		Governor	
	Vote for One		Vote for One
Amelia Earhart	<input type="radio"/>	Amelia Earhart	<input checked="" type="radio"/>
Howard Hughes	<input checked="" type="radio"/>	Howard Hughes	<input type="radio"/>
Charles Lindbergh	<input type="radio"/>	Charles Lindbergh	<input type="radio"/>
Write In	<input type="radio"/>	Write In	<input type="radio"/>

Fig. 5. Automatically moving voter marks—UnclearBallot seamlessly moves marks to the attacker’s preferred candidate while preserving the voter’s marking style. It is effective for a wide variety of marks and ballot designs. In the examples above, original ballot scans are shown on the left and manipulated images on the right.

By moving marks on each ballot separately, we ensure that the voter’s particular style of filling in an oval is preserved and consistent across the ballot. Figure 5 shows some marks swapped by our algorithm, and how the voters original mark is completely preserved in the process.

4.3 UnclearBallot

To illustrate the attack, we created UnclearBallot, a proof-of-concept implementation packaged as a malicious Windows scanner driver, which consists of 398 lines of C++ and Python. We tested it with a Fujitsu fi-7180 scanner (shown in Figure 6), which is federally certified for use in U.S. elections as part of Clear Ballot’s ClearVote system [43]. These scanners are typically used to handle small volumes of absentee ballots, and must be attached to a Windows workstation that runs the tabulation software.

The UnclearBallot driver wraps the stock scanner driver and alters images from the scanner before they reach the election management application. We chose this approach for simplicity, as the Windows driver stack is relatively easy



Fig. 6. The **Fujitsu fi-7180 scanner** we used to test our attack has been certified by the U.S. Election Assistance Commission for use in voting systems. Our proof-of-concept implementation is a malicious scanner driver that alters ballots on the fly.

to work with, but the attack could also be implemented at other layers of the computing stack. For instance, it could be even harder to detect if implemented as a malicious change to the scanner’s embedded firmware. Alternatively, it could be engineered as a modification to the tabulation software itself.

Once a ballot is scanned, the resulting bitmap is sent to our image processing software, which manipulates the ballot in the way described in Section 4.1. Prior to the election, the attacker specifies the ballot template, which race they would like to affect, and by how much. While ballots are being scanned, the software keeps a running tally of the actual ballot results, and changes ballot images on the fly to achieve the desired election outcome. To avoid detection, attackers can specify just enough manipulated images so that the race outcome is changed.

5 Evaluation

We evaluated the performance and effectiveness of UnclearBallot using two sets of experiments. In the first set of experiments, we marked different ballot styles by hand using types of marks taxonomized by Bajcsy et al. [2]. In the second set of experiments, we processed 181,541 ballots from the 2018 election in Clackamas County, Oregon.

5.1 Testing Across Ballot Styles

In order for our application to succeed at its goal (surreptitiously changing enough scanned ballots to achieve a chosen election outcome), it must be able to detect marks that constitute valid votes as well as distinguish marks which would be noticeable if moved. The marks in the latter case represent a larger set than just marginal marks, as they may indeed be completely valid votes, but considered invalid by our mark-moving algorithm. For example, if we were to swap the targets on a ballot where the user put a check through their target, we may leave a significant percentage of the check around the original target when swapping. The same applies for marked ballots where the filled in area extends into the candidate’s name, which could lead our algorithm to swap over parts of the candidate’s name when manipulating the image.

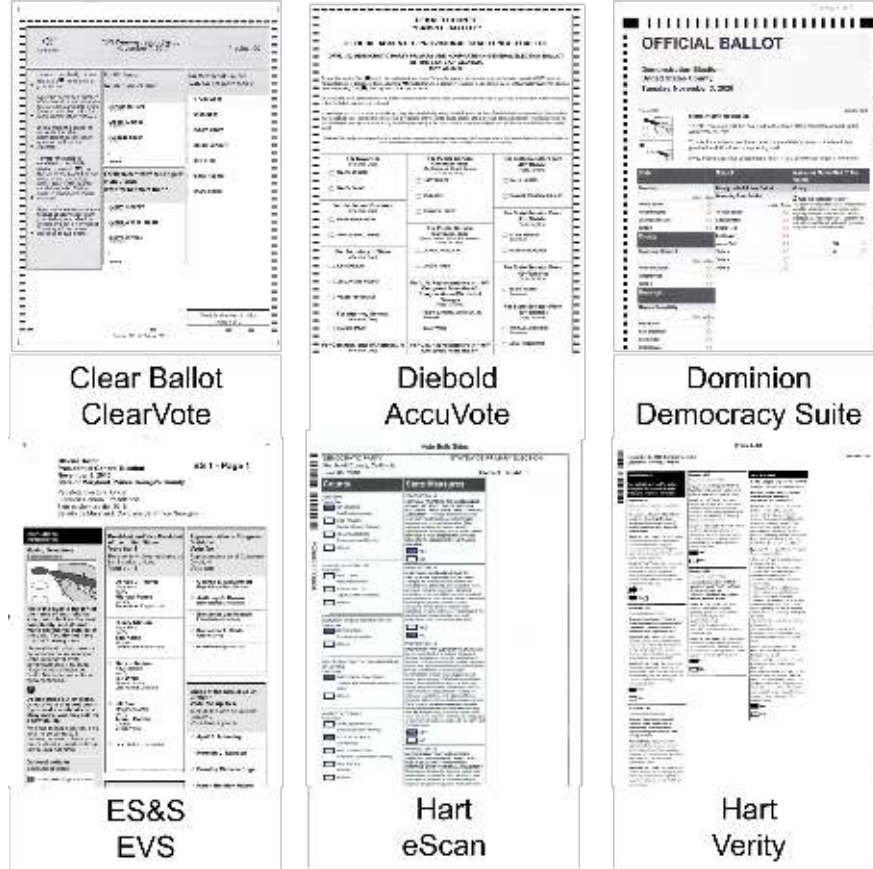


Fig. 7. Ballots Styles — We tested ballot designs from five U.S. voting system vendors: Clear Ballot, Diebold, Dominion, ES&S, and Hart (two styles, eScan and Verity).

To detect anomalies for invalid ballots, we leverage the same intensity checking algorithm that first found the marked areas. The program checks if the width or height is abnormally large, which would indicate an overfilled target, as well as if there are too few or too many areas of high intensity, which would indicate no target or too many targets are filled out. If the program detects an invalid ballot, it will not be modified by the program.

To show our attack is replicable on a variety of different ballot styles, we modified our program to work on six different sample ballot styles, shown in Figure 7. The ballots we tested come from the four largest election vendors in the U.S. (ES&S, Hart InterCivic, Dominion, and Clear Ballot), as well as two older styles of ballots from Hart and Diebold.

Our first experiment was designed to characterize the technique’s effectiveness across a range of ballot styles and with both regular and marginal marks. We

Ballot Style	Invalid Marks			Valid Marks			Time/Success
	Skipped	Success	Failure	Skipped	Success	Failure	
Clear Ballot	55	5	0	26	34	0	25 ms
Diebold	60	0	0	6	54	0	11 ms
Dominion	38	22	0	7	53	0	30 ms
ES&S	52	8	0	29	31	0	54 ms
Hart (eScan)	60	0	0	38	22	0	46 ms
Hart (Verity)	60	0	0	27	33	0	21 ms

Table 1. Performance of UnclearBallot — We tested how accurately our software could manipulate voter marks for a variety of ballot styles using equal numbers of invalid and valid marks. The table shows how often the system skipped a mark, successfully altered one, or erroneously created artifacts we deemed to be visible upon manual inspection. We also report the mean processing time for successfully manipulated races, excluding template matching.

prepared 720 marked contests, split evenly among the six ballot styles shown in Figure 7. For each style, we marked 60 contests with what Bajcsy [2] calls “Filled” marks, i.e. reliably detected marks that should be moved by our attack. We marked another 60 ballots in each ballot style with marginal marks, ten each for the five kinds of marginal marks shown in Figure 2 and ten empty marks.

Because the runtime of the template matching step of our algorithm is highly dependent on customization for the particular races on a ballot, we opted to skip it for this experiment. Rather than marking full ballots, we marked cropped races from each ballot style and then ran them through our program. We then manually checked to ensure that the races the program moved were not detectable by inspection. Results for these experiments are shown in Table 1.

Despite rejecting some valid ballots, our program is still able to confidently swap a majority of valid votes. In a real attack, only a small percentage of votes would need to actually be modified, a task easily accomplished by our program. Our program also correctly catches all votes that we have deemed invalid for swapping. This would make it unlikely to be detected in an image audit.

Dominion ballots saw a much higher rate of invalid mark moving, and Diebold and Dominion ballots saw a much higher rate of valid mark moving. This is likely due to the placement of targets: on the Dominion ballots, the mark is right justified, separating it significantly from candidate label information, as can be seen in Figure 7. Similarly, the Diebold ballot provides more space around the target and less candidate information that can be intercepted by marks, which would cause Unclear Ballot to skip moving the mark.

In an online attack scenario (such as if a human is waiting to see the output from the scanner), the attacker needs to be able to modify ballot scans quickly enough not to be noticed. Factors which might affect how quickly our program can process and manipulate ballots include ballot style, layout, and type of mark. During the accuracy experiment just described, we collected timing data for

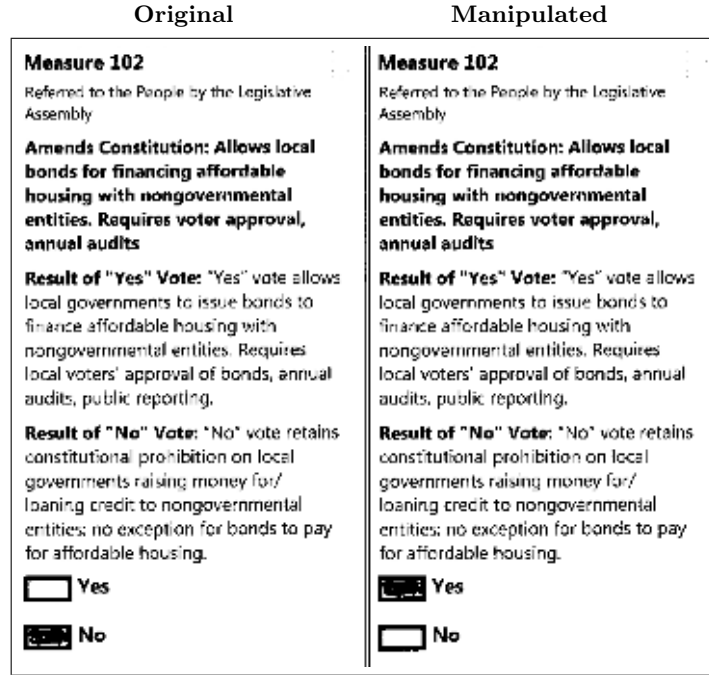


Fig. 8. Attacking Real Ballots—Using 181,541 images of voted ballots from Clackamas County, Oregon, we attempted to change voters’ selections for the ballot measure shown above. UnclearBallot determined that it could safely alter 34% of the ballots. For reference, Measure 102 passed by a margin of 5%, well within range of manipulation [14]. We inspected 1,000 of them to verify that the manipulation left no obvious artifacts.

successfully manipulated ballot, and report the results in Table 1. The results show that after the target race has been extracted, the algorithm completes extremely quickly for all tested ballot styles. We present additional timing data at the end of the following section.

5.2 Testing with Real Voted Ballots

To assess the effectiveness of UnclearBallot in a real election, we used a corpus of scans of 181,541 real ballots from the November 6, 2018, General Election in Clackamas County, Oregon, which were made available by Election Integrity Oregon [18]. Like all of Oregon, Clackamas County uses vote-by-mail as its primary voting method, and votes are centrally counted using optical scanners. All images were Hart Verity-style ballots, as shown in Figure 7.

We selected a ballot measure that appeared on all the ballots (Figure 8) and attempted to change each voter’s selection. UnclearBallot rejected 20,117 (11%) of the ballots because it could not locate the target contest. We examined a subset of the rejected ballots and found that they contained glitches introduced

during scanning (such as vertical lines running the length of the ballot), which interfered with the Hough transform.

To simulate a real attacker, we configured UnclearBallot with conservative parameters, so that it would only modify marks when there was high confidence that the alteration would not be noticeable. As a result, it would only manipulate marks that were nearly perfectly filled in. In most cases, marks that were skipped extended well beyond the target, but the program also skipped undervotes, overvotes, or mislabeled scans. Under these parameters, the program altered the target contest in 62,400 (34%) of the ballot images.

Two authors independently inspected a random sample of 1,000 altered ballots to check whether any contained artifacts that would be noticeable to an attentive observer. Such artifacts might include marks which were unnaturally cut off, visible discontinuities in pixel darkness (i.e. dark lines around moved marks), and so on. If these artifacts were seen during an audit, officials might recheck all of the physical ballots and reverse the effects of the attack. None of the altered ballots we inspected contained noticeable evidence of manipulation.

We also collected timing data while processing Clackamas County ballots. Running on a system with a 4-core Intel E3-1230 CPU running at 3.40 GHz with 64 GB of RAM, UnclearBallot took an average of 279 ms to process each ballot. For reference, Hart’s fastest central scanner’s maximum scan rate is one ballot per 352 ms [37], well above the time needed to carry out our attack.

These results show that UnclearBallot can successfully and efficiently manipulate ballot images to change real voters’ marks. Moreover, the alterations likely would be undetectable to human auditors who examined only the ballot images.

6 Discussion and Mitigations

UnclearBallot demonstrates the need for a software-independent evidence trail against which election results can be checked. It shows that audits based on software which is independent from the rest of the election system is still not software independent. To date, the only robust and secure election technology that is widely used is optical-scan paper ballots with risk-limiting audits based on a robust, well-maintained, *physical* audit trail. However, image audits are not useless, and here we discuss uses for them as well as potential mitigations for our attack.

Uses for image audits. So long as image audits are not the sole mechanism for verifying election results, they do provide substantial benefits to election officials. Using an image audit vastly simplifies some functions of election administration, like ballot adjudication in cases where marks cannot be interpreted by scanners or are otherwise ambiguous. Image audits can be used to efficiently identify and document election discrepancies, as has occurred in Maryland where nearly 2,000 ballots were discovered missing from the audit trail in 2016 [28]. Image audits also identified a flaw in the ES&S DS850 high speed scanner, where it was causing some ballots to stick together and feed two at a time [29].

Another way to utilize image audits is a transitive audit. Methods like SOBA [8] seek to construct an audit trail using all available means of election evidence, rooting the audit in some verification of physical record. By using physical records to verify other records, like CVRs or ballot images, confidence in election outcomes can be transitively passed on to non-physical audit trails. The drawback with this kind of audit is that it usually requires the same level of work as an RLA, plus whatever work is needed to validate the other forms of evidence. However, since ballot image audits already require a low amount of effort, they may augment RLAs and provide better transparency into the auditing process.

Image audits are an augmentation and a convenience for election administration, however, and should not be viewed as a security tool. Only physical examination of paper ballots, as in a risk-limiting audit, can provide a necessary level of mitigation to manipulated election results.

End-to-end (E2E) systems. Voting systems with rigorous integrity properties and tamper resistance such as Scantegrity [12] and Prêt à Voter [35] provide a defense to UnclearBallot. In Scantegrity, when individuals mark their ballots, a confirmation code is revealed that is tied to the selected candidate. This enables a voter to verify that their ballot collected-as-cast and counted-as-collected, as they can look up their ballot on a public bulletin board. Since each mark reveals a unique code, moving the mark would match the code with the wrong candidate, so voters would be unable to verify their ballots. If enough voters complain, this might result in our attack being detected.

Prêt à Voter randomizes the candidate order on each ballot, which creates a slightly higher barrier for our attack, as an additional template matching step would be needed to ascertain candidate order. More importantly, the candidate list is physically separated from the voter’s marks upon casting the ballot, so malware which could not keep track of the correct candidate order could not successfully move marks to a predetermined candidate. Since the candidate order is deciphered via a key-sharing scheme, malicious software would have to infect a significant portion of the election system and act in a highly coordinated way to reconstruct candidate ordering. Moreover, as with Scantegrity, votes are published to a public bulletin board, so any voter could discover if their vote had not been correctly recorded.

Other E2E systems which make use of optical scanning and a bulletin board, like STAR-Vote [6], Scratch and Vote [1], and VeriScan [7], are similarly protected from attacks like UnclearBallot.

Other mitigations. Outside of E2E, there may be other heuristic mitigations that can be easily implemented even in deployed voting systems to make our attack somewhat more difficult. As mentioned above, randomizing candidate order on each ballot increases the computation required to perform our attack. Voters drawing outside the bubbles can also defeat our attack, though this might also result in their votes not counting and may be circumvented by replacing the whole race on the ballot image with a substituted one. Collecting ballot images

from a different source than the tabulator makes our attack more difficult, as votes now have to be changed in two places. Other standard computer security technologies, like secure file systems, could be used to force the attacker to alter ballot images in a way that also circumvents protections like encryption and permissions.

Detection. Technologies that detect image manipulation may also provide some mitigation. Techniques like those discussed in [3–5, 38], among others, could be adapted to try to automatically detect moved marks on ballots. However, as noted by Farid [19], image manipulation detection is a kind of arms race: given a fixed detection algorithm, adversaries can very likely find a way to defeat it. In our context, an attacker with sufficient access to the voting system to implant a manipulation algorithm would likely also be able to steal the detector code. The attacker could improve the manipulation algorithm or simply use the detector as part of their mark-moving calculus: if moving a mark will trip the detector, an attacker can simply opt not to move the mark.

While a fixed and automatic procedure for detecting manipulation can provide little assurance, it remains possible that an adaptive approach to detection could be a useful part of a post-election forensics investigation. However, staying one step ahead of sophisticated adversaries would require an ongoing research program to advance the state of the art in detection methods.

A less costly and more dependable way to detect ballot manipulation detection would be to use a software independent audit trail to confirm election outcomes. This can be accomplished with risk-limiting audits, and the software independence enabled by RLAs provides other robust security properties to elections, including defending against other potential attacks on tabulation equipment and servers.

Future work. We have only focused on simple-majority elections here, because those are the kinds of elections used by jurisdictions that do image audits. Audits of more complex election methods, like instant-runoff voting or D’Hondt, have been examined to some extent [36, 41], but future work is needed into audits of these kinds of elections altogether. Because the marks made in these elections are different than the kind we’ve discussed here, manipulating these ballot images may not be able to employ the same image processing techniques we have used. Additionally it may be difficult for malware to know how many marks it needs to move, since margins in complex elections are difficult to compute. We leave exploration of image manipulation of these elections to future work.

7 Conclusion

In this paper, we demonstrated an attack that defeats ballot image audits of the type performed in some jurisdictions. We presented an implementation using a real scanner, and evaluated our implementation against a set of real ballots and a set of systematically marked ballots from a variety of ballot styles. Our

attack shows that image audits cannot be relied upon to verify that elections are free from computer-based interference. Indeed, the only currently known way to verify an election outcome is with direct examination of physical ballots.

Acknowledgements

The authors thank Vaibhav Bafna and Jonathan Yan for assisting in the initial version of this project. They also thank Josh Franklin, Joe Hall, Maurice Turner, Kevin Skoglund, Jared Marcotte, and Tony Adams for their invaluable feedback. We also thank our anonymous reviewers and our shepherd, Roland Wen. This material is based upon work supported by the National Science Foundation under grant CNS-1518888.

References

1. Adida, B., Rivest, R.L.: Scratch and Vote: Self-contained paper-based cryptographic voting. In: ACM Workshop on Privacy in the Electronic Society. pp. 29–40 (2006)
2. Bajcsy, A., Li-Baboud, Y.S., Brady, M.: Systematic measurement of marginal mark types on voting ballots. Tech. rep., National Institute for Standards and Technology (2015)
3. Bayar, B., Stamm, M.C.: A deep learning approach to universal image manipulation detection using a new convolutional layer. In: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. pp. 5–10. ACM (2016)
4. Bayram, S., Avcibas, I., Sankur, B., Memon, N.: Image manipulation detection with binary similarity measures. In: 2005 13th European Signal Processing Conference. pp. 1–4. IEEE (2005)
5. Bayram, S., Avcibas, I., Sankur, B., Memon, N.D.: Image manipulation detection. *Journal of Electronic Imaging* **15**(4), 041102 (2006)
6. Bell, S., Benaloh, J., Byrne, M.D., DeBeauvoir, D., Eakin, B., Fisher, G., Kortum, P., McBurnett, N., Montoya, J., Parker, M., Pereira, O., Stark, P.B., Wallach, D.S., Winn, M.: STAR-vote: A secure, transparent, auditable, and reliable voting system. *USENIX Journal of Election Technology and Systems* **1**(1) (Aug 2013)
7. Benaloh, J.: Administrative and public verifiability: Can we have both? In: *USENIX/ACCURATE Electronic Voting Technology Workshop. EVT '08* (Aug 2008)
8. Benaloh, J., Jones, D., Lazarus, E., Lindeman, M., Stark, P.B.: SOBA: Secrecy-preserving observable ballot-level audit. In: *proc. Proc. USENIXAccurate Electronic Voting Technology Workshop* (2011)
9. Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y., Stark, P.B., Teague, V., Vora, P.L., Wallach, D.S.: Public evidence from secret ballots. In: *International Joint Conference on Electronic Voting*. pp. 84–109. Springer (2017)
10. Bowen, D.: Top-to-Bottom Review of voting machines certified for use in California. Tech. rep., California Secretary of State (2007), <https://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/>
11. Bradski, G.: The OpenCV Library. *Dr. Dobb's Journal of Software Tools* (2000)
12. Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy. In: *18th USENIX Security Symposium* (Aug 2010)

13. Chung, K.K.t., Dong, V.J., Shi, X.: Electronic voting method for optically scanned ballot (Jul 18 2006), US Patent 7,077,313
14. November 6, 2018 general election. <https://dochub.clackamas.us/documents/drupal/f4e7f0fb-250a-4992-918d-26c5f726de3c>
15. Clear Ballot: ClearAudit, <https://clearballot.com/products/clear-audit>
16. Dominion Voting: Auditmark. <https://www.dominionvoting.com/pdf/DD%20Digital%20Ballot%20AuditMark.pdf>
17. Dominion Voting: Cambridge Case Study. <https://www.dominionvoting.com/field/cambridge>
18. Election Integrity Oregon, <https://www.electionintegrityoregon.org>
19. Farid, H.: Digital forensics in a post-truth age. *Forensic science international* **289**, 268–269 (2018)
20. Feldman, A.J., Halderman, J.A., Felten, E.W.: Security analysis of the Diebold AccuVote-TS voting machine. In: USENIX/ACCURATE Electronic Voting Technology Workshop. EVT '07 (Aug 2007)
21. Hall, J., Miratrix, L., Stark, P., Briones, M., Ginnold, E., Oakley, F., Peaden, M., Pellerin, G., Stanionis, T., Webber, T.: Implementing risk-limiting post-election audits in California. In: 2009 Workshop on Electronic Voting Technology/Workshop on Trustworthy Elections. pp. 19–19. USENIX Association (2009)
22. Ji, T., Kim, E., Srikantan, R., Tsai, A., Cordero, A., Wagner, D.A.: An analysis of write-in marks on optical scan ballots. In: EVT/WOTE (2011)
23. Jones, D.W.: On optical mark-sense scanning. In: Towards Trustworthy Elections, pp. 175–190. Springer (2010)
24. Lindeman, M., Halvorson, M., Smith, P., Garland, L., Addona, V., McCrea, D.: Principles and best practices for post-election audits (Sep 2008), <http://electionaudits.org/files/bestpracticesfinal.0.pdf>
25. Lindeman, M., Stark, P.: A gentle introduction to risk-limiting audits. *IEEE Security and Privacy* **10**, 42–49 (2012)
26. Lindeman, M., Stark, P., Yates, V.: BRAVO: Ballot-polling risk-limiting audits to verify outcomes. In: 2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '12). USENIX (2012)
27. Maryland House of Delegates: House Bill 1278: An act concerning election law – postelection tabulation audit. <http://mgaleg.maryland.gov/2018RS/bills/hb/hb1278E.pdf>
28. Maryland State Board of Elections: 2016 post-election audit report. http://dlslibrary.state.md.us/publications/JCR/2016/2016_22-23.pdf (12 2016)
29. Maryland State Board of Elections: December 15, 2016 meeting minutes. <https://elections.maryland.gov/pdf/minutes/2016.12.pdf> (Dec 2016)
30. McDaniel, P., Blaze, M., Vigna, G.: EVEREST: Evaluation and validation of election-related equipment, standards and testing. Tech. rep., Ohio Secretary of State (2007), <http://siis.cse.psu.edu/everest.html>
31. Mebane, W., Bernhard, M.: Voting technologies, recount methods and votes in Wisconsin and Michigan in 2016. 3rd Workshop on Advances in Secure Electronic Voting 2018 (2018)
32. National Academies of Sciences, Engineering, and Medicine: Securing the Vote: Protecting American Democracy. The National Academies Press, Washington, DC (2018), <https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy>
33. National Conference of State Legislatures: Post-election audits (January 2019), <http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>

34. Rivest, R.: On the notion of ‘software independence’ in voting systems. *Phil. Trans. R. Soc. A* **366**(1881), 3759–3767 (October 2008)
35. Ryan, P.Y.A., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à Voter: A voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security* **4**(4), 662–673 (2009)
36. Sarwate, A.D., Checkoway, S., Shacham, H.: Risk-limiting audits and the margin of victory in nonplurality elections. *Statistics, Politics and Policy* **4**(1), 29–64 (2013)
37. ScannerOne: Kodak i5600. <http://www.scannerone.com/product/KOD-i5600.html>
38. Stamm, M.C., Liu, K.R.: Forensic detection of image manipulation using statistical intrinsic fingerprints. *IEEE Transactions on Information Forensics and Security* **5**(3), 492–506 (2010)
39. Stark, P.: Conservative statistical post-election audits. *Ann. Appl. Stat.* **2**(2), 550–581 (2008)
40. Stark, P.: Super-simple simultaneous single-ballot risk-limiting audits. In: 2010 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE ’10). *USENIX* (2010)
41. Stark, P.B., Teague, V., Essex, A.: Verifiable European elections: Risk-limiting audits for D’Hondt and its relatives. *USENIX Journal of Election Technology and Systems (JETS)* **1**, 18–39 (2014)
42. Unisyn Voting Solutions: OpenElect OCS Auditor. <https://unisynvoting.com/openelect-ocs/>
43. U.S. Election Assistance Commission: Certificate of conformance: ClearVote 1.5. <https://www.eac.gov/file.aspx?A=zgte4IhsHz%2bswC%2bW4LO6PxIVssxXBebhvZiSd5BGbbs%3d> (2019)
44. Verified Voting Foundation: The Verifier: Polling place equipment (2019), <https://www.verifiedvoting.org/verifier/>

From: [Shekinah Cantere](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Testimony for Elections Commission meeting on Fri 9/16 at 10am
Date: Friday, September 16, 2022 10:02:55 AM

Aloha,

I would like to just share my concerns that I have with our elections process. I know first hand people that have received their mail in ballots to vote here in Maui that no longer live here. I am also aware that people receive multiple ballots or the wrong ballots if they have changed addresses.

There are many flaws in today's mail in ballot system.

In person here in Maui, the staff running the voting centers also had people fill out an Affidavit. This was required or else you weren't allowed to vote. To me this process seemed to discourage in person voting since it would make the process longer and I believe their also needs to be signage posted outside of voting centers letting people know that if they are turning in their mail in ballots then there is a separate line for that.

I believe ID's should be checked for every mail in ballot received.

Mahalo for your consideration,

Shekinah Cantere