DATE FILED: December 17, 2021 11:53 AM
FILING ID: BC329FCB8936E
CASE NUMBER: 2020CV34319

EXHIBIT 11 A

The State of Texas

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

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

Ruth R. Hughs
Secretary of State

REPORT OF REVIEW OF DOMINION VOTING SYSTEMS DEMOCRACY SUITE 5.5-A

PRELIMINARY STATEMENT

On October 2-3, 2019, Dominion Voting Systems ("Dominion" or the "Vendor") presented the Democracy Suite 5.5-A system for examination and certification. The examination was conducted in Austin, Texas. Pursuant to Sections 122.035(a) and (b) of the Texas Election Code, the Secretary of State appointed the following examiners:

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

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

1. Dr. Jim Sneeringer, an expert in electronic data communication systems; and
2. Mr. Ryan Vassar, an employee of the Texas Attorney General.

On October 2, 2019, Mr. Pinney, Mr. Mechler, and Dr. Sneeringer witnessed the installation of the Democracy Suite 5.5-A software and firmware that the Office of the Texas Secretary of State (the "Office") received directly from the Independent Testing Authority. The next day, Mr. Pinney examined the accessibility components of the ImageCast X Ballot Marking Device.

On October 3, 2019, the Vendor demonstrated the Democracy Suite 5.5-A system and answered questions presented by the examiners. Test ballots were then processed on each voting device. The results were accumulated and later verified for accuracy by staff of the Secretary of State.

Examiner reports regarding the Democracy Suite 5.5-A system are attached hereto and incorporated herein by this reference.

On December 27, 2019, pursuant to Section 122.0371 of the Texas Election Code, the Office held a public hearing for interested persons to express views for or against the certification of the Democracy Suite 5.5-A system.

BRIEF DESCRIPTION OF DEMOCRACY SUITE 5.5-A

The Democracy Suite 5.5-A system is an updated version of the Democracy Suite 5.5 system, which was denied certification by the Office on June 20, 2019. The Democracy Suite 5.5-A system includes certain software and hardware updates to the Suite 5.5 version.

Democracy Suite 5.5-A has been evaluated at an accredited independent voting system laboratory for conformance to the 2005 Voluntary Voting System Guidelines (VVSG). Democracy Suite 5.5-A was certified by the Election Assistance Commission (EAC) on January 30, 2019.

The components of Democracy Suite 5.5-A are as follows:

Component	Version	Description
EMS – Election Management System	5.5.12.1	Election Management System
ADJ – Adjudication	5.5.8.1	
ICC – ImageCast Central	5.5.3.0002	Central scanner
ICX – ImageCast X BMD	5.5.10.30	Ballot marking device
ICP – ImageCast Precinct	5.5.3-0002	Precinct scanner

FINDINGS

The following are the findings, based on written evidence submitted by the Vendor in support of its application for certification, oral evidence presented at the examination, and the findings of the voting system examiners as set out in their written reports.

The examiner reports identified multiple hardware and software issues that preclude the Office of the Texas Secretary of State from determining that the Democracy Suite 5.5-A system satisfies each of the voting-system requirements set forth in the Texas Election Code. Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation. Therefore, the Democracy Suite 5.5-A system and corresponding hardware devices do not meet the standards for certification prescribed by Section 122.001 of the Texas Election Code.

CONCLUSION

Accordingly, based upon the foregoing, I hereby deny certification of Dominion Voting Systems' Democracy Suite 5.5-A system for use in Texas elections.

Signed under my hand and seal of office, this 24th day of January 2020.

JOSE A. ESPARZA
DEPUTY SECRETARY OF STATE

EXHIBIT 11 B

The State of Texas

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

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

Ruth R. Hughs
Secretary of State

REPORT OF REVIEW OF DOMINION VOTING SYSTEMS DEMOCRACY SUITE 5.5-A

PRELIMINARY STATEMENT

On October 2-3, 2019, Dominion Voting Systems ("Dominion" or the "Vendor") presented the Democracy Suite 5.5-A system for examination and certification. The examination was conducted in Austin, Texas. Pursuant to Sections 122.035(a) and (b) of the Texas Election Code, the Secretary of State appointed the following examiners:

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

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

1. Dr. Jim Sneeringer, an expert in electronic data communication systems; and
2. Mr. Ryan Vassar, an employee of the Texas Attorney General.

On October 2, 2019, Mr. Pinney, Mr. Mechler, and Dr. Sneeringer witnessed the installation of the Democracy Suite 5.5-A software and firmware that the Office of the Texas Secretary of State (the "Office") received directly from the Independent Testing Authority. The next day, Mr. Pinney examined the accessibility components of the ImageCast X Ballot Marking Device.

On October 3, 2019, the Vendor demonstrated the Democracy Suite 5.5-A system and answered questions presented by the examiners. Test ballots were then processed on each voting device. The results were accumulated and later verified for accuracy by staff of the Secretary of State.

Examiner reports regarding the Democracy Suite 5.5-A system are attached hereto and incorporated herein by this reference.

BRIEF DESCRIPTION OF DEMOCRACY SUITE 5.5-A

The Democracy Suite 5.5-A system is an updated version of the Democracy Suite 5.5 system, which was denied certification by the Office on June 20, 2019. The Democracy Suite 5.5-A system includes certain software and hardware updates to the Suite 5.5 version.

Democracy Suite 5.5-A has been evaluated at an accredited independent voting system laboratory for conformance to the 2005 Voluntary Voting System Guidelines (VVSG). Democracy Suite 5.5-A was certified by the Election Assistance Commission (EAC) on January 30, 2019.

The components of Democracy Suite 5.5-A are as follows:

Component	Version	Description
EMS – Election Management System	5.5.12.1	Election Management System
ADJ – Adjudication	5.5.8.1	
ICC – ImageCast Central	5.5.3.0002	Central scanner
ICX – ImageCast X BMD	5.5.10.30	Ballot marking device
ICP – ImageCast Precinct	5.5.3-0002	Precinct scanner

FINDINGS

The following are the findings, based on written evidence submitted by the Vendor in support of its application for certification, oral evidence presented at the examination, and the findings of the voting system examiners as set out in their written reports.

The examiner reports identified multiple hardware and software issues that preclude the Office of the Texas Secretary of State from determining that the Democracy Suite 5.5-A system satisfies each of the voting-system requirements set forth in the Texas Election Code. Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation. Therefore, the Democracy Suite 5.5-A system and corresponding hardware devices do not meet the standards for certification prescribed by Section 122.001 of the Texas Election Code.

CONCLUSION

Accordingly, based upon the foregoing, I hereby deny certification of Dominion Voting Systems' Democracy Suite 5.5-A system for use in Texas elections.

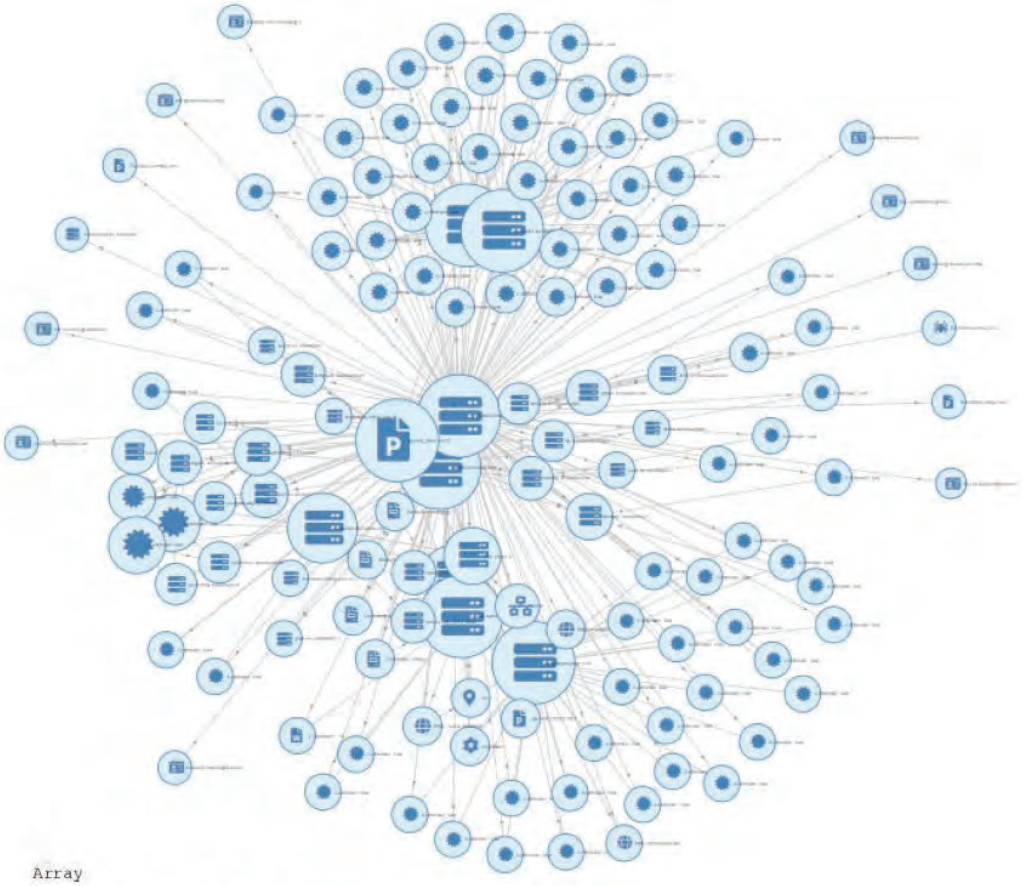
Signed under my hand and seal of office, this 24th day of January 2020.

JOSE A. ESPARZA
DEPUTY SECRETARY OF STATE

EXHIBIT 12

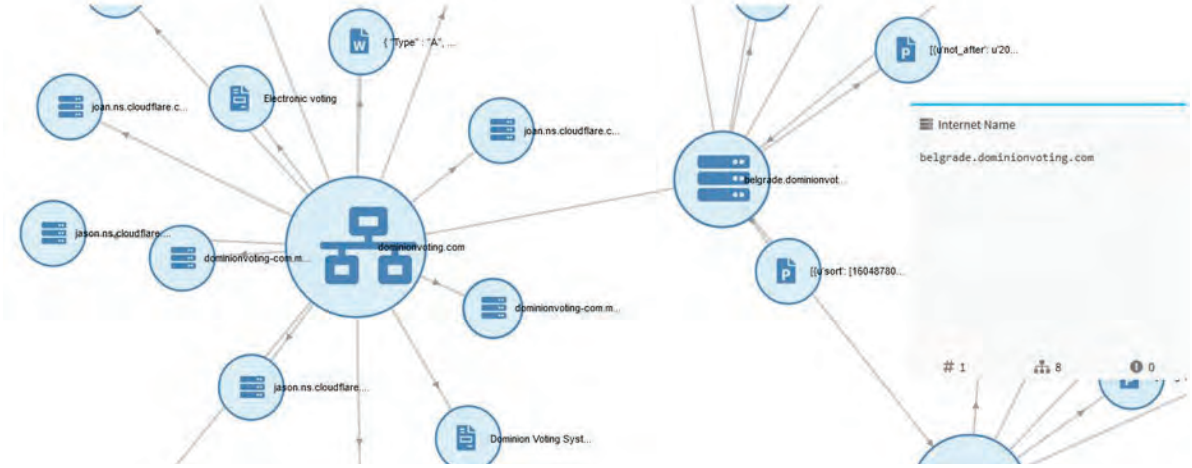
Declaration of [redacted]
Pursuant to 28 U.S.C Section 1746, [redacted] make the following declaration.

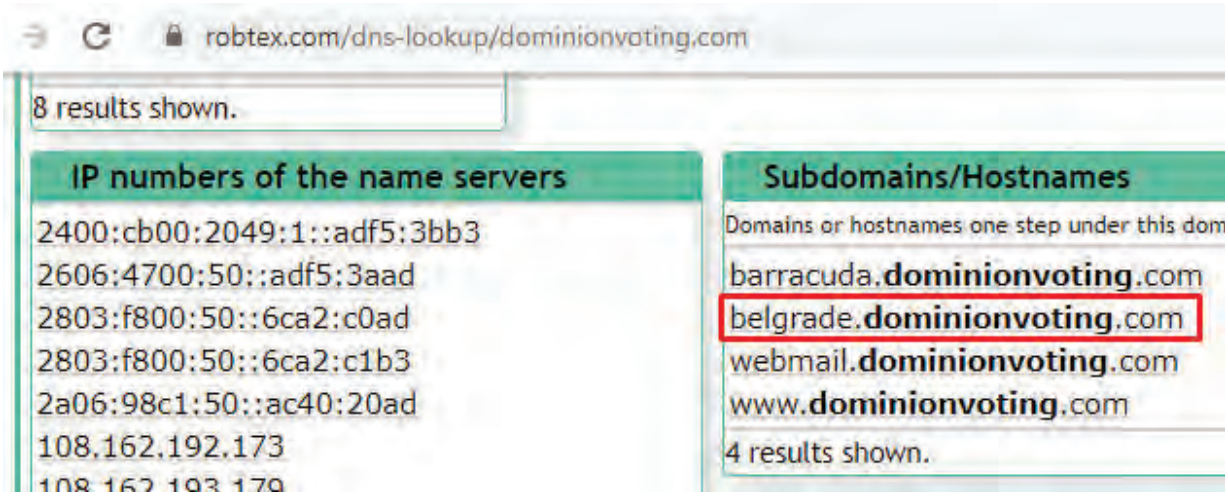
1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I was an electronic intelligence analyst under 305th Military Intelligence with experience gathering SAM missile system electronic intelligence. I have extensive experience as a white hat hacker used by some of the top election specialists in the world. The methodologies I have employed represent industry standard cyber operation toolkits for digital forensics and OSINT, which are commonly used to certify connections between servers, network nodes and other digital properties and probe to network system vulnerabilities.
3. I am a US citizen and I reside [redacted] location in the United States of America.
4. Whereas the Dominion and Edison Research systems exist in the internet of things, and whereas this makes the network connections between the Dominion, Edison Research and related network nodes available for scanning,
5. And whereas Edison Research's primary job is to report the tabulation of the count of the ballot information as received from the tabulation software, to provide to Decision HQ for election results,
6. And whereas Spiderfoot and Robtex are industry standard digital forensic tools for evaluation network security and infrastructure, these tools were used to conduct public security scans of the aforementioned Dominion and Edison Research systems,
7. A public network scan of Dominionvoting.com on 2020-11-08 revealed the following inter-relationships and revealed 13 unencrypted passwords for dominion employees, and 75 hashed passwords available in TOR nodes:



```
Array
(
    [id] => 544167324
    [luser] => ian.macvicar
    [domain] => dominionvoting.com
    [password] => jamley
)

7
Array
(
    [id] => 599400504
    [luser] => jelena.tanaskovic
    [domain] => dominionvoting.com
```

8. The same public scan also showed a direct connection to the group in Belgrade as highlighted below:

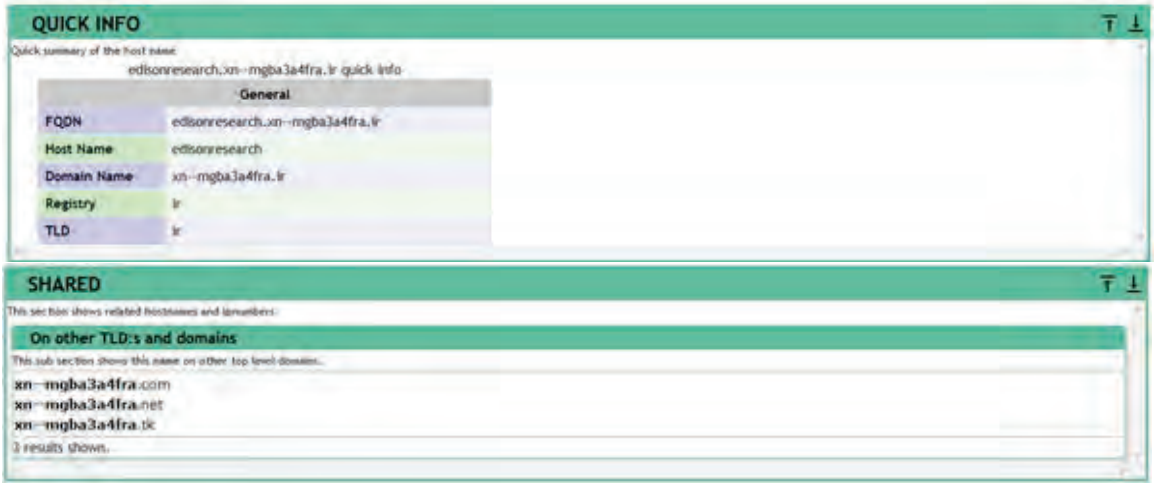




9. A cursory search on LinkedIn of "dominion voting" on 11/19/2020 confirms the numerous employees in Serbia:

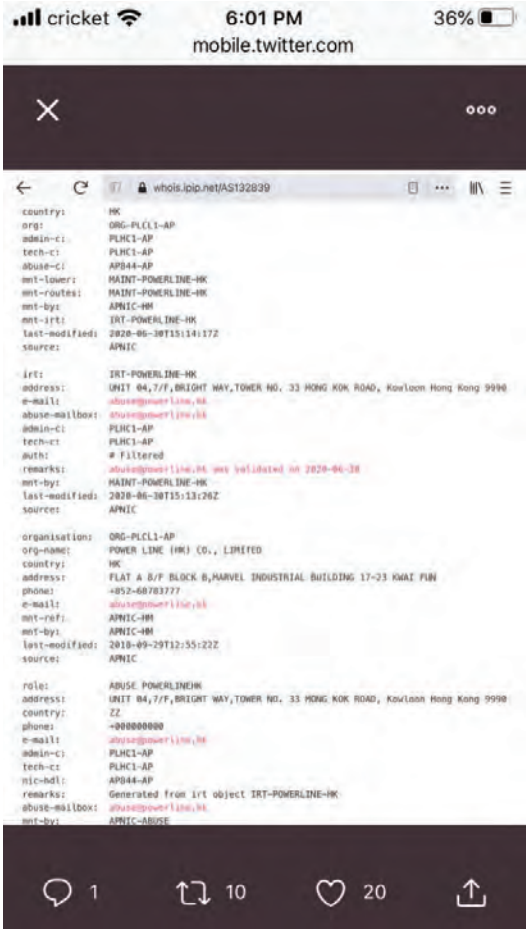
10. An additional search of Edison Research on 2020-11-08 showed that Edison Research has an Iranian server seen here:

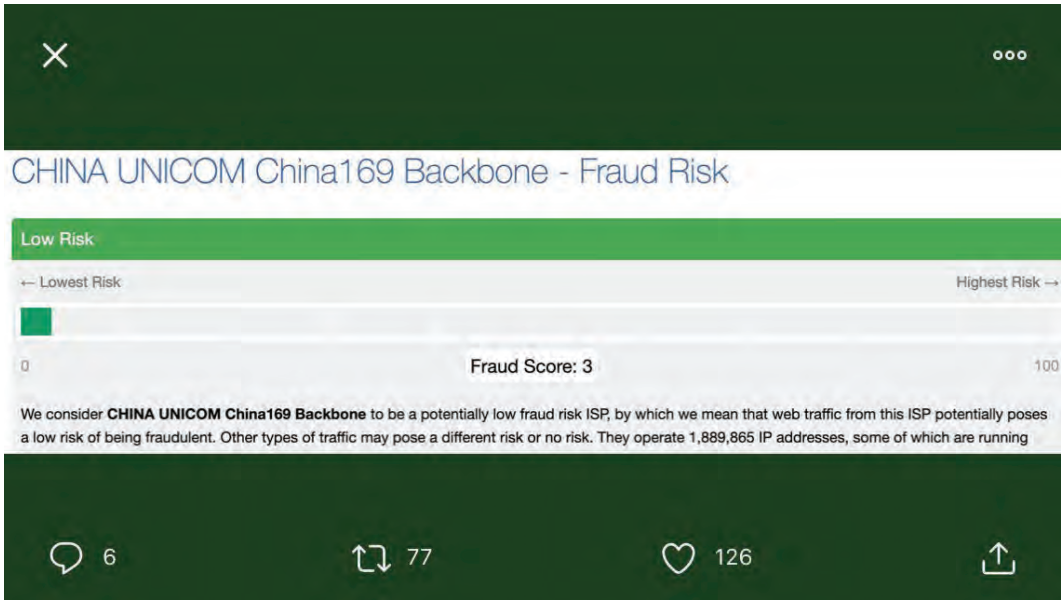
Inputting the Iranian IP into Robtex confirms the direct connection into the "edisonresearch" host from the perspective of the Iranian domain also. This means that it is not possible that the connection was a unidirectional reference.



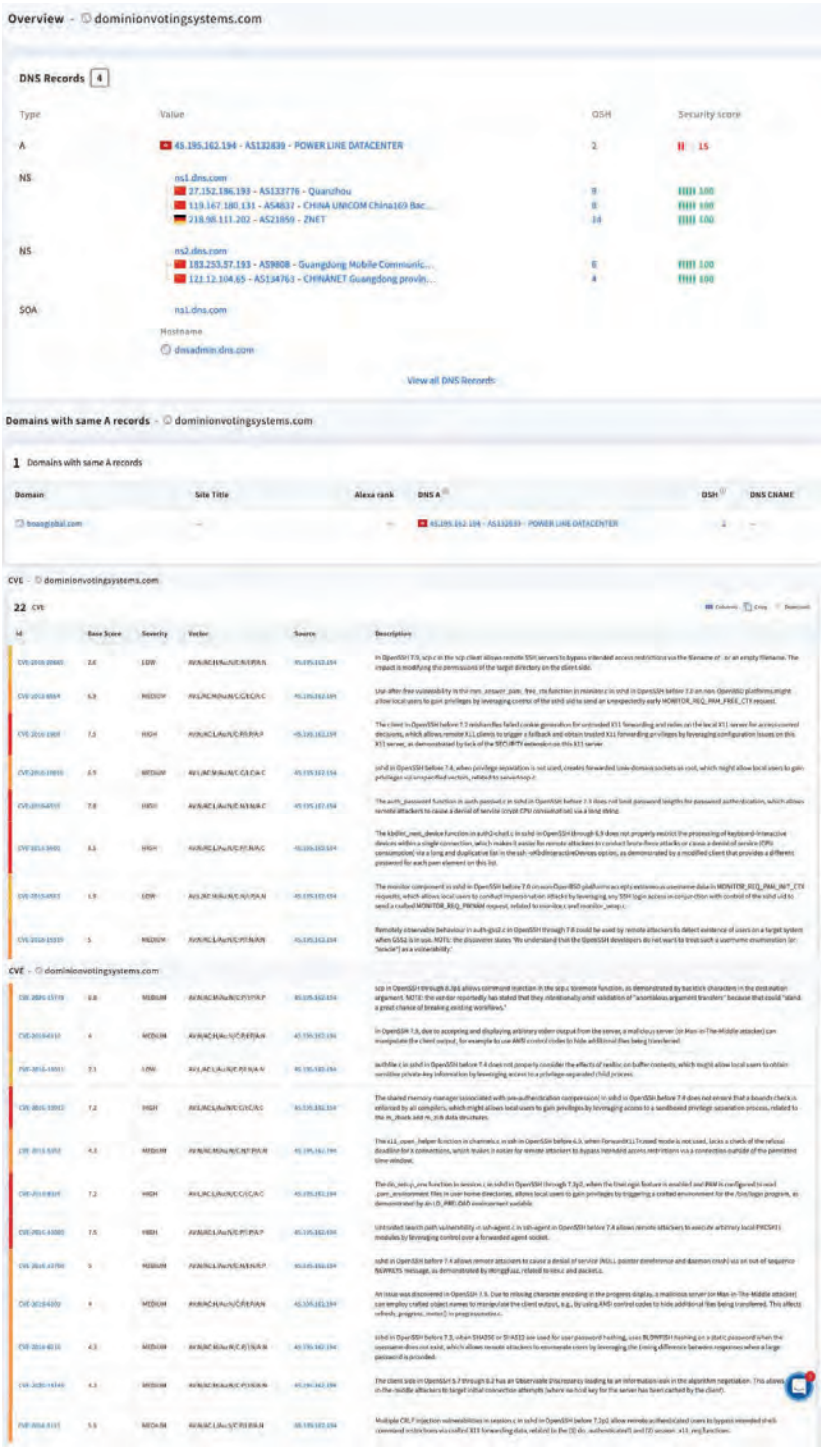
A deeper search of the ownership of Edison Research "edisonresearch.com" shows a connection to BMA Capital Management, where shareofear.com and bmacapital.com are both connected to edisonresearch.com via a VPS or Virtual Private Server, as denoted by the "vps" at the start of the internet name:

Dominionvoting is also dominionvotingsystems.com, of which there are also many more examples, including access of the network from China. The records of China accessing the server are reliable.





Domain Name: dominionvotingsystems.com
Registry Domain ID: 2530599738_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-05-26T15:48:58Z
Creation Date: 2020-05-26T15:48:57Z
Registrar Registration Expiration Date: 2021-05-26T15:48:57Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Hunan
Registrant Country: CN
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com
Name Server: NS1.DNS.COM
Name Server: NS2.DNS.COM
DNSSEC: unsigned



11. BMA Capital Management is known as a company that provides Iran access to capital markets with direct links publicly discoverable on LinkedIn (found via google on 11/19/2020):

www.linkedin.com › muhammad-talha-a0759660

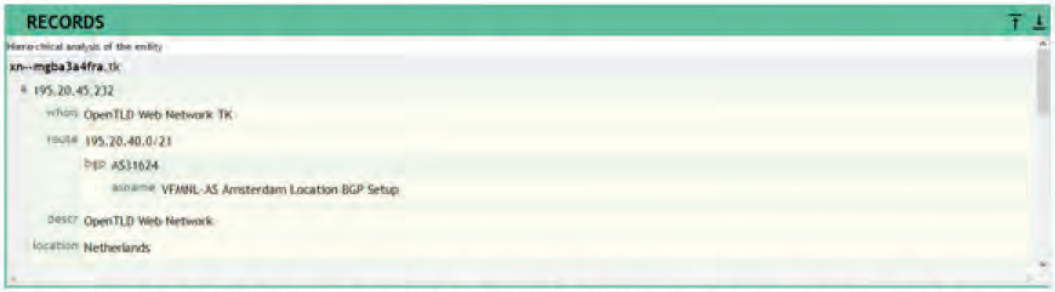
Muhammad Talha - BMA Capital Management Limited

Manager, Money Market & Fixed Income at **BMA Capital** Management Limited. **BMA Capital** ...

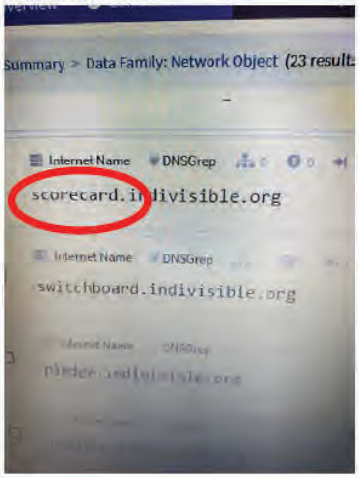
Manager-FMR at Pak **Iran** Joint Investment Company. Pakistan.

Pakistan · Manager, Money Market & Fixed Income · BMA Capital Management Limited

The same Robtex search confirms the Iranian address is tied to the server in the Netherlands, which correlates to known OSINT of Iranian use of the Netherlands as a remote server (See Advanced Persistent Threats: APT33 and APT34):

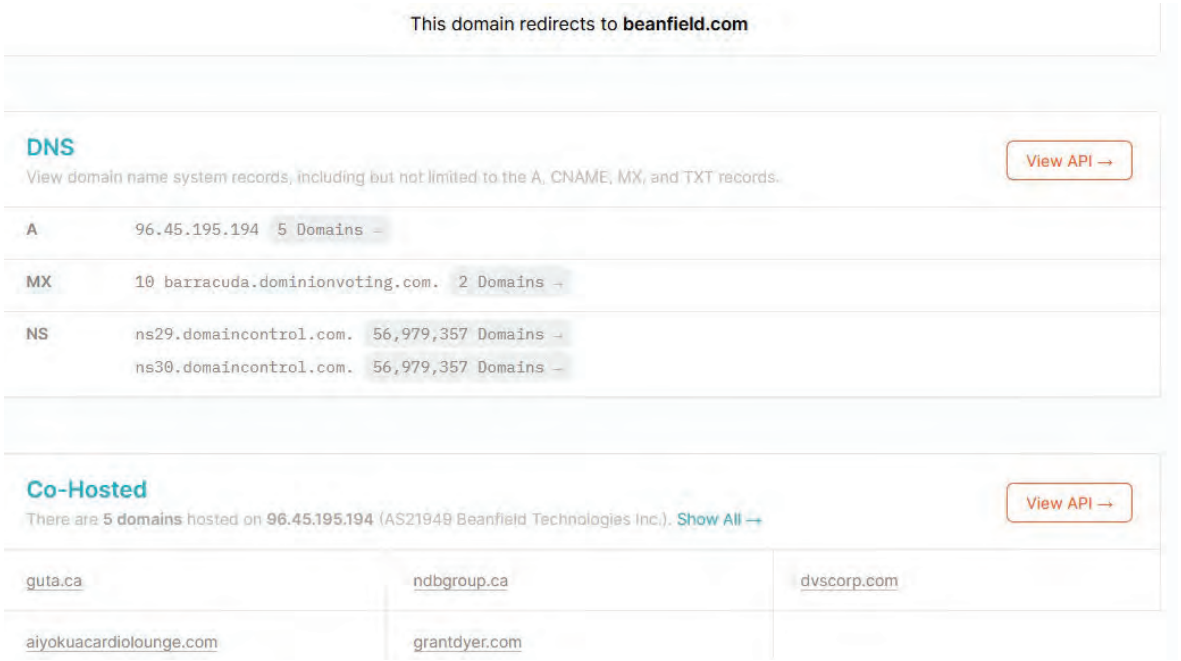


12. A search of the indivisible.org network showed a subdomain which evidences the existence of scorecard software in use as part of the Indivisible (formerly ACORN) political group for Obama:

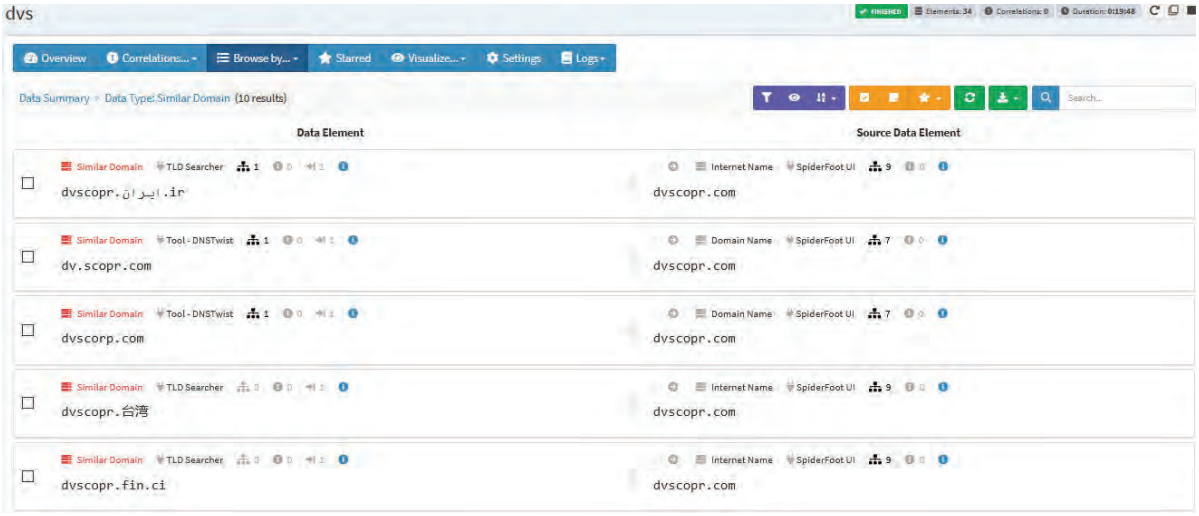


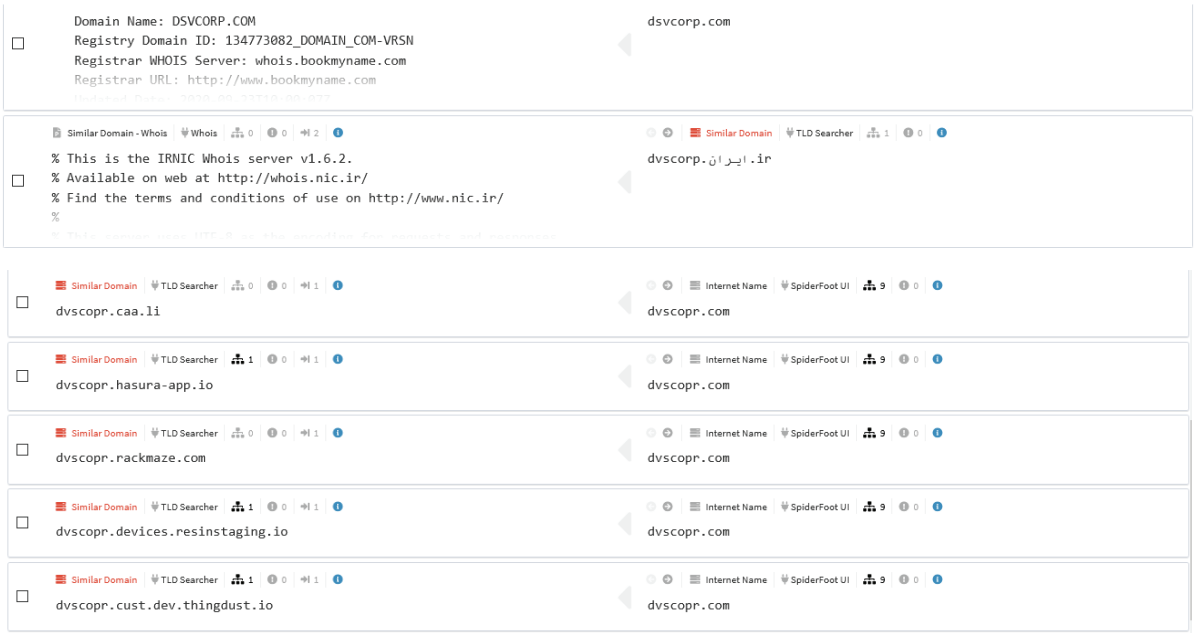
13. Each of the tabulation software companies have their own central reporting "affiliate". Edison Research is the affiliate for Dominion.

14. Beanfield.com out of Canada shows the connections via co-hosting related sites, including dvscorp.com:



This Dominion partner domain "dvscorp" also includes an auto discovery feature, where new in-network devices automatically connect to the system. The following diagram shows some of the related dvscopr.com mappings, which mimic the infrastructure for Dominion and are an obvious typo derivation of the name. Typo derivations are commonly purchased to catch redirect traffic and sometimes are used as honeypots. The diagram shows that infrastructure spans multiple different servers as a methodology.





The above diagram shows how these domains also show the connection to Iran and other places, including the following Chinese domain, highlighted below:

15. The auto discovery feature allows programmers to access any system while it is connected to the internet once it's a part of the constellation of devices (see original Spiderfoot graph).
16. Dominion Voting Systems Corporation in 2019 sold a number of their patents to China (via HSBC Bank in Canada):

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame	Execution date	Date recorded	Pages
050500/0236	Sep 25, 2019	Sep 26, 2019	7

Conveyance

SECURITY AGREEMENT

Assignors	Correspondent	Attorney docket
DOMINION VOTING SYSTEMS CORPORATION	CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020	

Assignee

HSBC BANK CANADA, AS COLLATERAL AGENT

4TH FLOOR, 70 YORK STREET

TORONTO M5J 1S9

CANADA

Properties (18)

Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195505	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		
7422151	20070012767	11526028		
D599131		29324281		

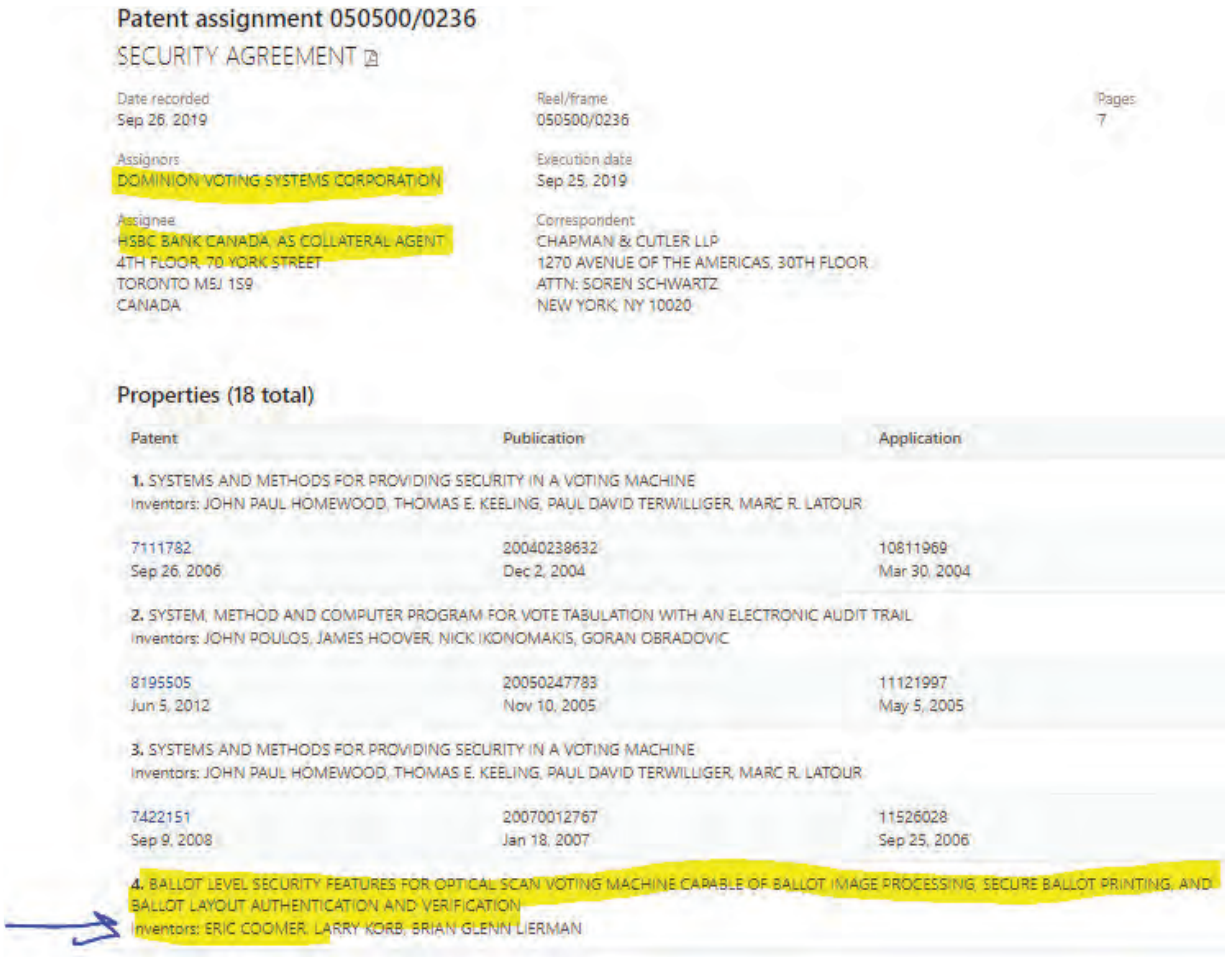
View all

This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function–the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

Release 2.0.0 | Release Notes | Send Feedback | Legacy Patent Assignment Search | Legacy Trademark Assignment Search

Of particular interest is a section of the document showing aspects of the nature of the patents dealing with authentication:



Patent assignment 050500/0236

SECURITY AGREEMENT

Date recorded	Reel/frame	Pages
Sep 26, 2019	050500/0236	7

Assignors
DOMINION VOTING SYSTEMS CORPORATION

Execution date
Sep 25, 2019

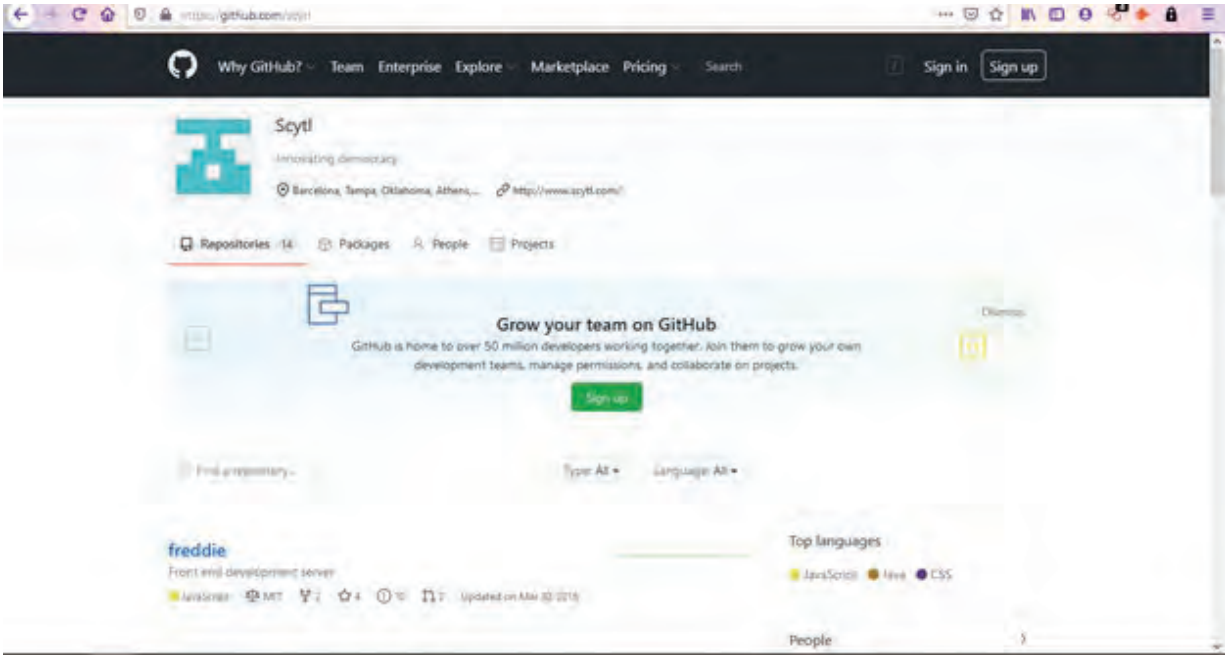
Assignee
HSBC BANK CANADA, AS COLLATERAL AGENT
4TH FLOOR, 70 YORK STREET
TORONTO M5J 1S9
CANADA

Correspondent
CHAPMAN & CUTLER LLP
1270 AVENUE OF THE AMERICAS, 30TH FLOOR
ATTN: SOREN SCHWARTZ
NEW YORK, NY 10020

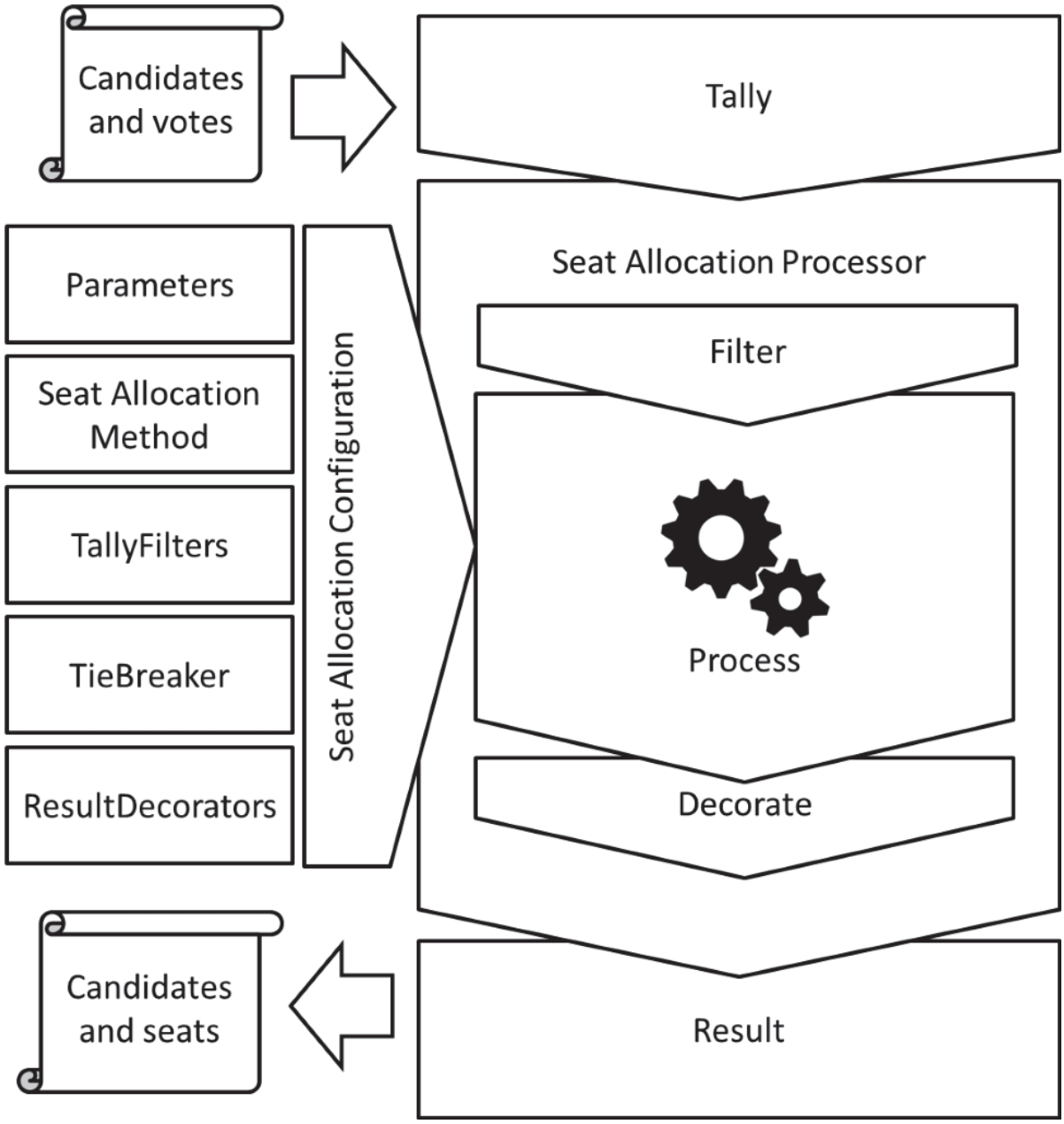
Properties (18 total)

Patent	Publication	Application
1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7111782 Sep 26, 2006	20040238632 Dec 2, 2004	10811969 Mar 30, 2004
2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL Inventors: JOHN POULOS, JAMES HOOVER, NICK IKONOMAKIS, GORAN OBRADOVIC		
8195505 Jun 5, 2012	20050247783 Nov 10, 2005	11121997 May 5, 2005
3. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7422151 Sep 9, 2008	20070012767 Jan 18, 2007	11526028 Sep 25, 2006
4. BALLOT LEVEL SECURITY FEATURES FOR OPTICAL SCAN VOTING MACHINE CAPABLE OF BALLOT IMAGE PROCESSING, SECURE BALLOT PRINTING, AND BALLOT LAYOUT AUTHENTICATION AND VERIFICATION Inventors: ERIC COOMER, LARRY KORB, BRIAN GLENN LIERMAN		

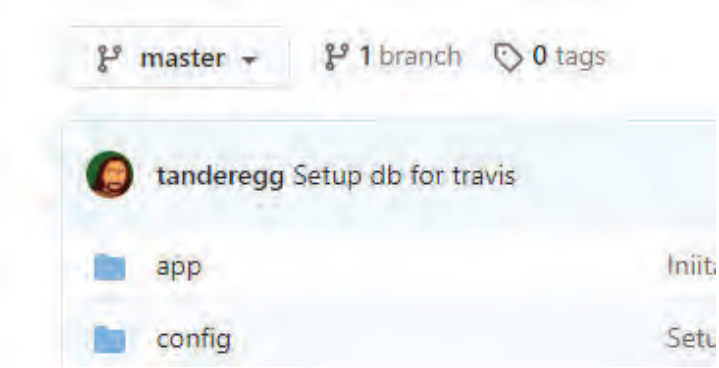
17. Smartmatic creates the backbone (like the cloud). SCYTL is responsible for the security within the election system.



18. In the GitHub account for Scytl, Scytl Jseats has some of the programming necessary to support a much broader set of election types, including a decorator process where the data is smoothed, see the following diagram provided in their source code:



19. Unrelated, but also a point of interest is CTCL or Center for Tech and Civic Life funded by Mark Zuckerberg. Within their github page (https://github.com/ctcl), one of the programmers holds a government position. The Bipcoop repo shows tanderegg as one of the developers, and he works at the Consumer Financial Protection Bureau:



20. As seen in included document titled "AA20-304A-Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data " that was authored by the Cybersecurity & Infrastructure Security Agency (CISA) with a Product ID of AA20-304A on a specified date of October 30, 2020, CISA and the FBI reports that Iranian APT teams were seen using ACUTENIX, a website scanning software, to find vulnerabilities within Election company websites, confirmed to be used by the Iranian APT teams buy seized cloud storage that I had personally captured and reported to higher authorities. These scanning behaviors showed that foreign agents of aggressor nations had access to US voter lists, and had done so recently.
21. In my professional opinion, this affidavit presents unambiguous evidence that Dominion Voter Systems and Edison Research have been accessible and were certainly compromised by rogue actors, such as Iran and China. By using servers and employees connected with rogue actors and hostile foreign influences combined with numerous easily discoverable leaked credentials, these organizations neglectfully allowed foreign adversaries to access data

and intentionally provided access to their infrastructure in order to monitor and manipulate elections, including the most recent one in 2020. This represents a complete failure of their duty to provide basic cyber security. This is not a technological issue, but rather a governance and basic security issue: if it is not corrected, future elections in the United States and beyond will not be secure and citizens will not have confidence in the results.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this November 23th, 2020.

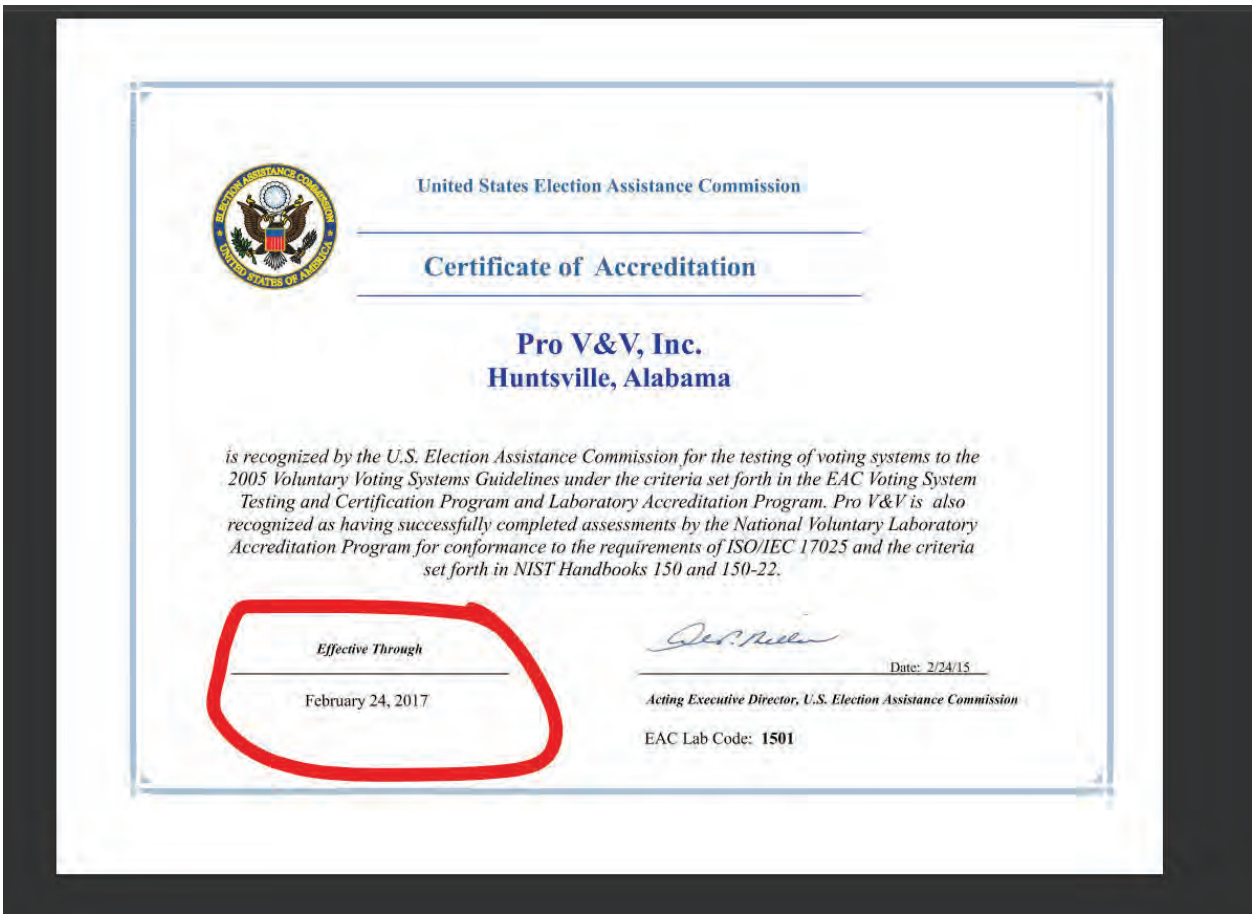
EXHIBIT 13

Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted], 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.



United States Election Assistance Commission

Certificate of Accreditation

Pro V&V, Inc.
Huntsville, Alabama

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2005 Voluntary Voting Systems Guidelines under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. Pro V&V is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Effective Through

February 24, 2017

Date: 2/24/15

Acting Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

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.

10. 

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

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 Communique dated January 2009).

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

For the National Voluntary Laboratory Accreditation Program

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).

U.S. Election Assistance Commission

MICHIGAN

State Participation:	**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.
Applicable Statute(s):	"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).
Applicable Regulation(s):	MI does not have a regulation regarding the federal certification process.
State Certification Process:	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).
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.michigan.gov/sos/0,1607,7-127-1633_8716_45458---,00.html

13.

WISCONSIN

State Participation:	**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.
Applicable Statute(s):	"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).
Applicable Regulation(s):	"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).
State Certification Process:	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).
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://elections.state.wi.us/section.asp?linkid=643&locid=47

14.

U.S. Election Assistance Commission

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/

15.

U.S. Election Assistance Commission

PENNSYVANIA

State Participation:	**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.
Applicable Statute(s):	"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).
Applicable Regulation(s):	PA does not have a regulation regarding the federal certification process.
State Certification Process:	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).
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.votespa.com/HowtoVote/tabid/74/language/en-US/Default.aspx

16.

U.S. Election Assistance Commission

ARIZONA

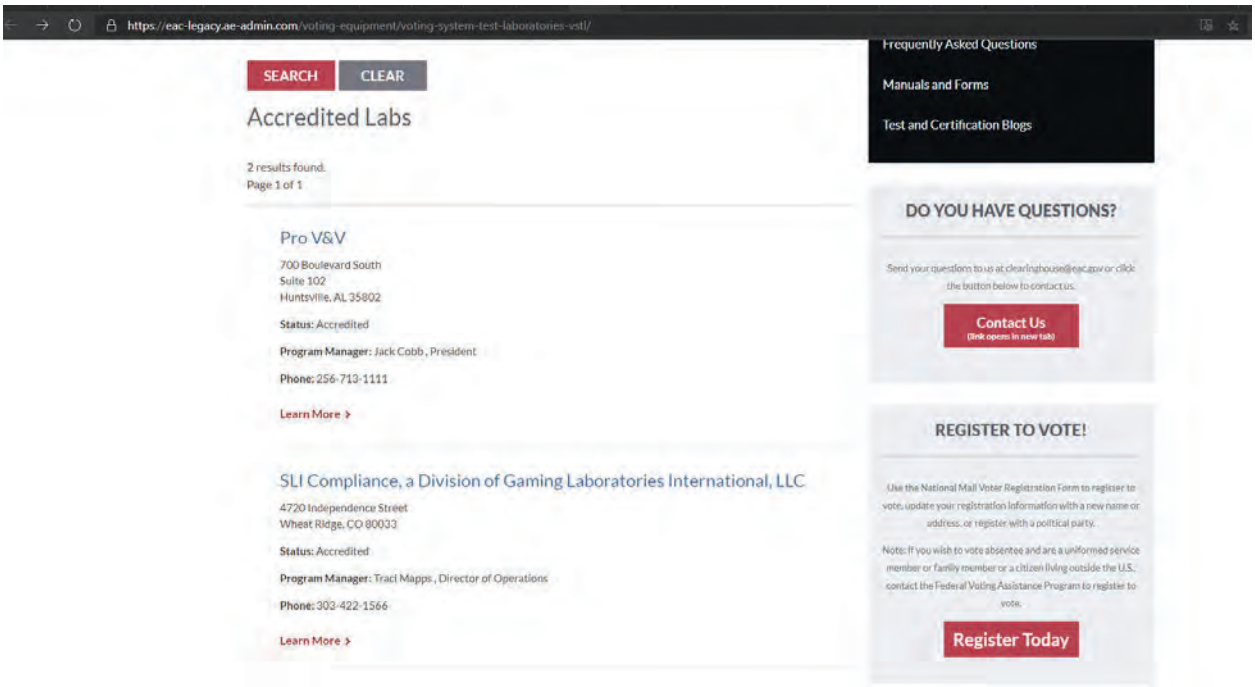
State Participation:	**Requires Testing by a Federally Accredited Laboratory.** AZ requires that its voting systems are HAVA compliant and approved by a laboratory that is accredited pursuant to HAVA.
Applicable Statute(s):	"On completion of acquisition of machines or devices that comply with HAVA, machines 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).
Applicable Regulation(s):	AZ does not have a regulation regarding the federal certification process.
State Certification Process:	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).
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.azsos.gov/election/equipment/default.htm

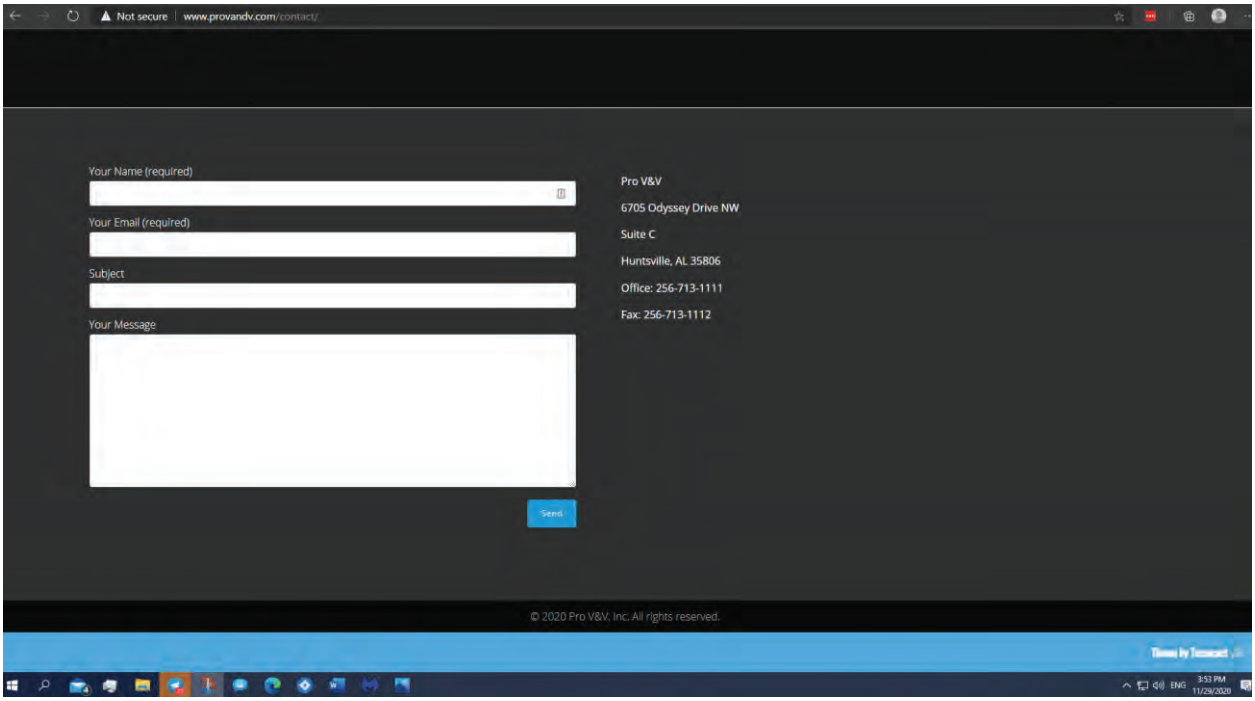
State Participation in EAC Voting System Certification Program 9

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. They 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

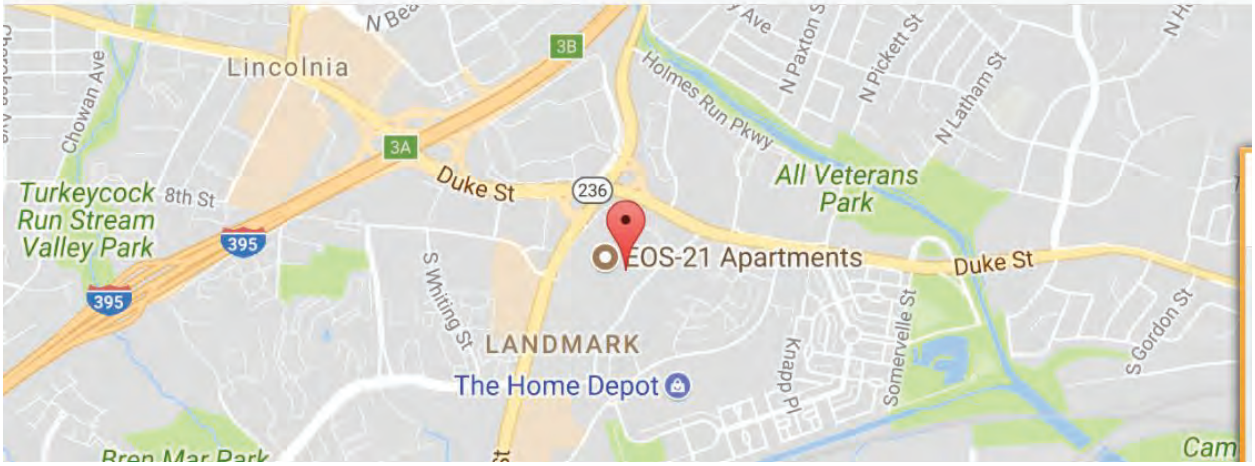
Akamai Technologies - Singapore
Akamai, Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
Driving directions
Telephone: +65 6248 4614
Fax: +65 6248-4501
Regional Manager: Stuart Spiteri

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

27.

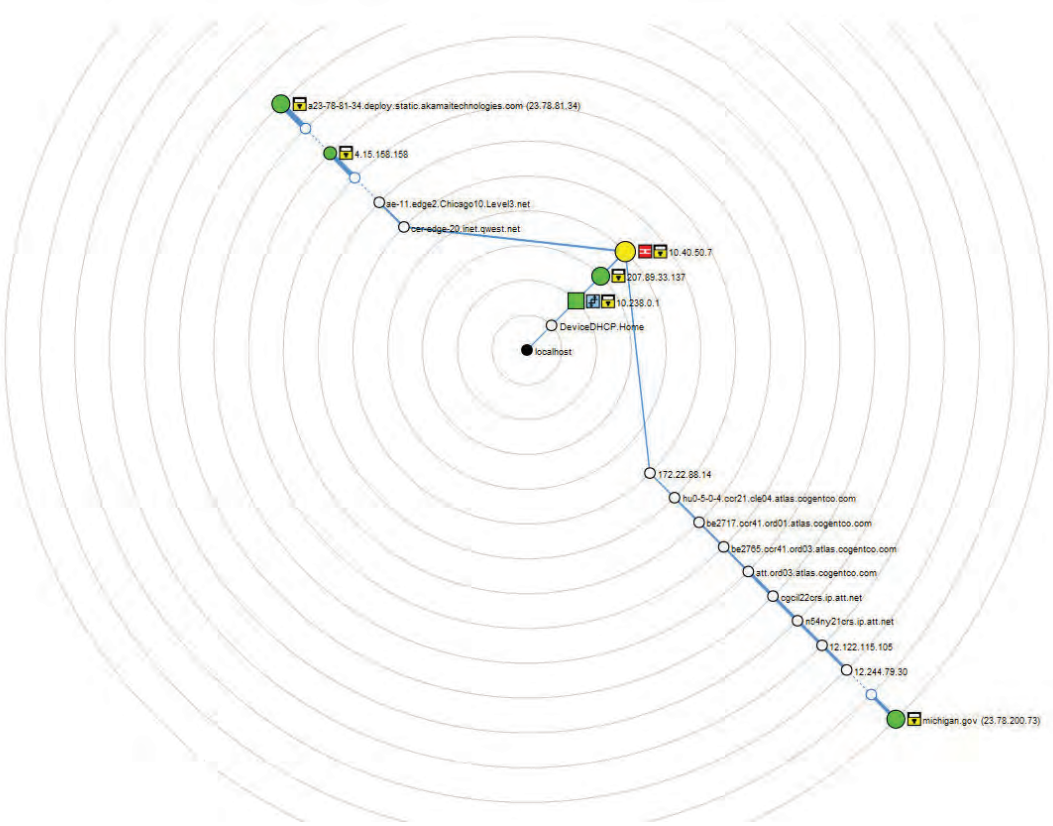
ptt.gov resolves to 4.30.228.74. According to our data this IP address belongs to *Level 3 Communications* and is located in *Alexandria, Virginia, United States*. Please have a look at the information provided below for further details.

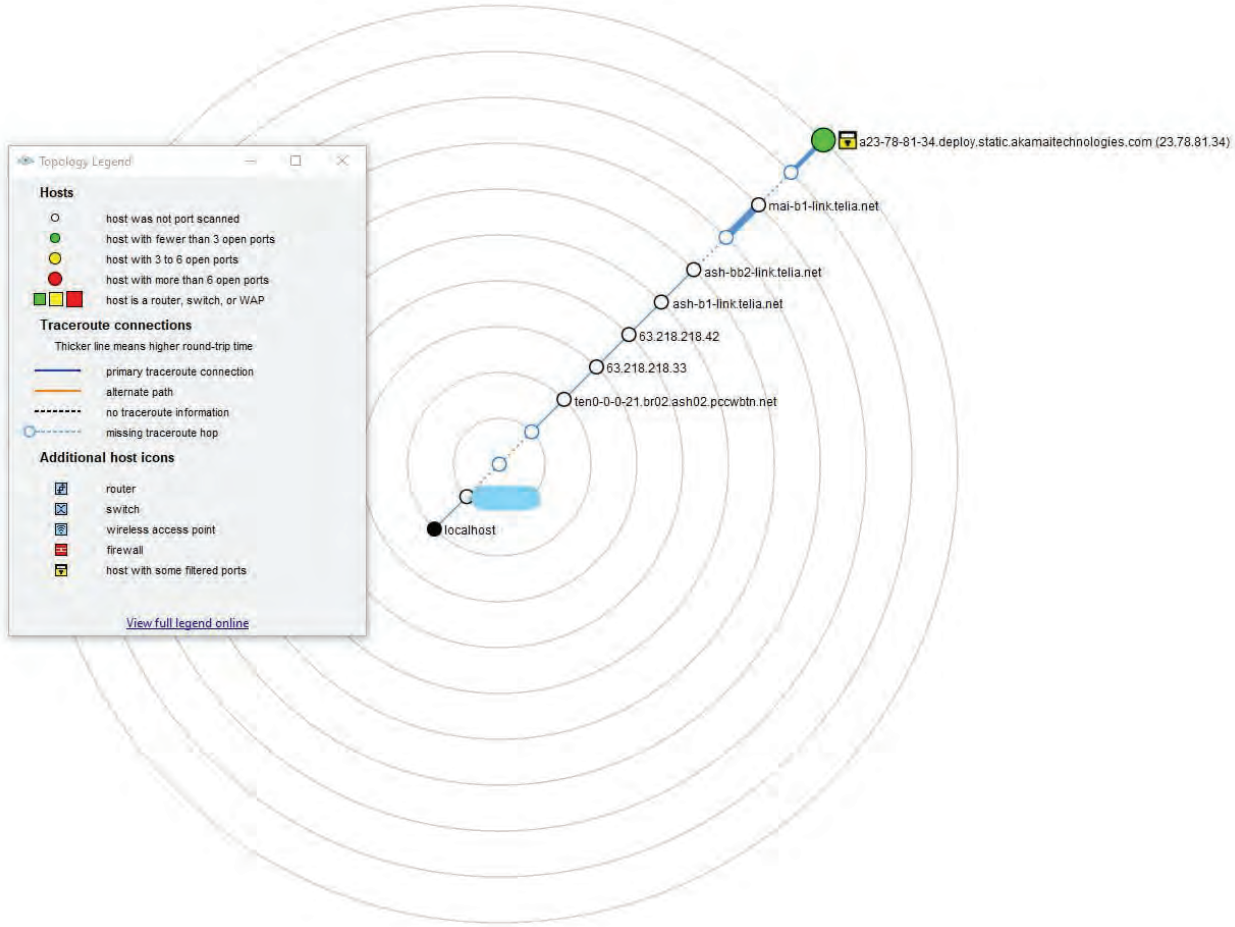
4.30.228.74	
ISP/Organization	Level 3 Communications
Location	Alexandria 22304, Virginia (VA), United States (US)
Latitude	38.8115 / 38°48'41" N
Longitude	-77.1285 / 77°7'42" W
Timezone	America/New_York
Local Time	Thu, 12 Jul 2018 19:27:40 -0400



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.

29.


a23-78-81-34.deploy.static.akamaitechnologies.com (23.78.81.34)
4.15.158.158
ae-11.edge2.Chicago10.Level3.net
cer-edge-20.inet.qwest.net
10.40.50.7
207.89.33.137
10.238.0.1
DeviceDHCP.Home
localhost
172.22.88.14
hu0-5-0-4.ccr21.cle04.atlas.cogentco.com
be2717.ccr41.ord01.atlas.cogentco.com
be2765.ccr41.ord03.atlas.cogentco.com
att.ord03.atlas.cogentco.com
cgcil22crs.ip.att.net
n54ny21crs.ip.att.net
12.122.115.105
12.244.79.30
michigan.gov (23.78.200.73)



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
	Nameservers:	a12-67.akam.net >> 184.26.160.67 a11-66.akam.net >> 84.53.139.66 a1-35.akam.net >> 193.108.91.35 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 : 1.4.1Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-Aconsists 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 Scytl (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 a 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

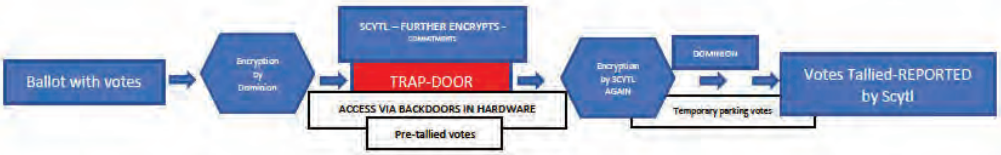
- Setup: Group $\mathcal{G}$ of prime order q with generator g
- Public key: $pk = y = g^x$
- Encryption: $\mathcal{E}_{pk}(m; r) = (g^r, y^r m)$
- Decryption: $\mathcal{D}_x(u, v) = vu^{-x}$
- Homomorphic:

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

- Re-rencryption:

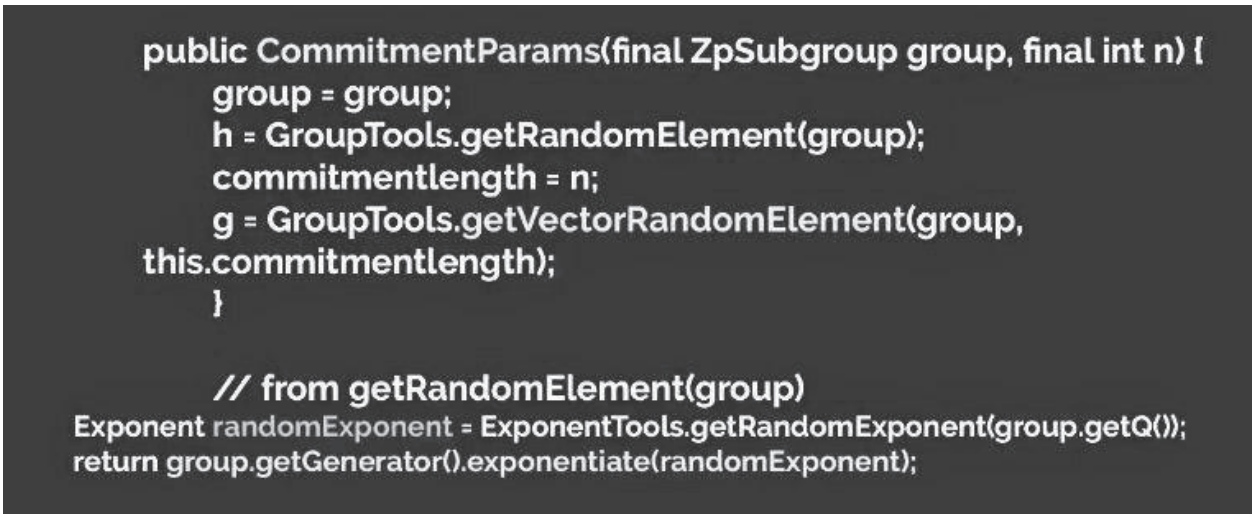
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(1; R) = \mathcal{E}_{pk}(m; r + R)$$

UCL

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).
51. 

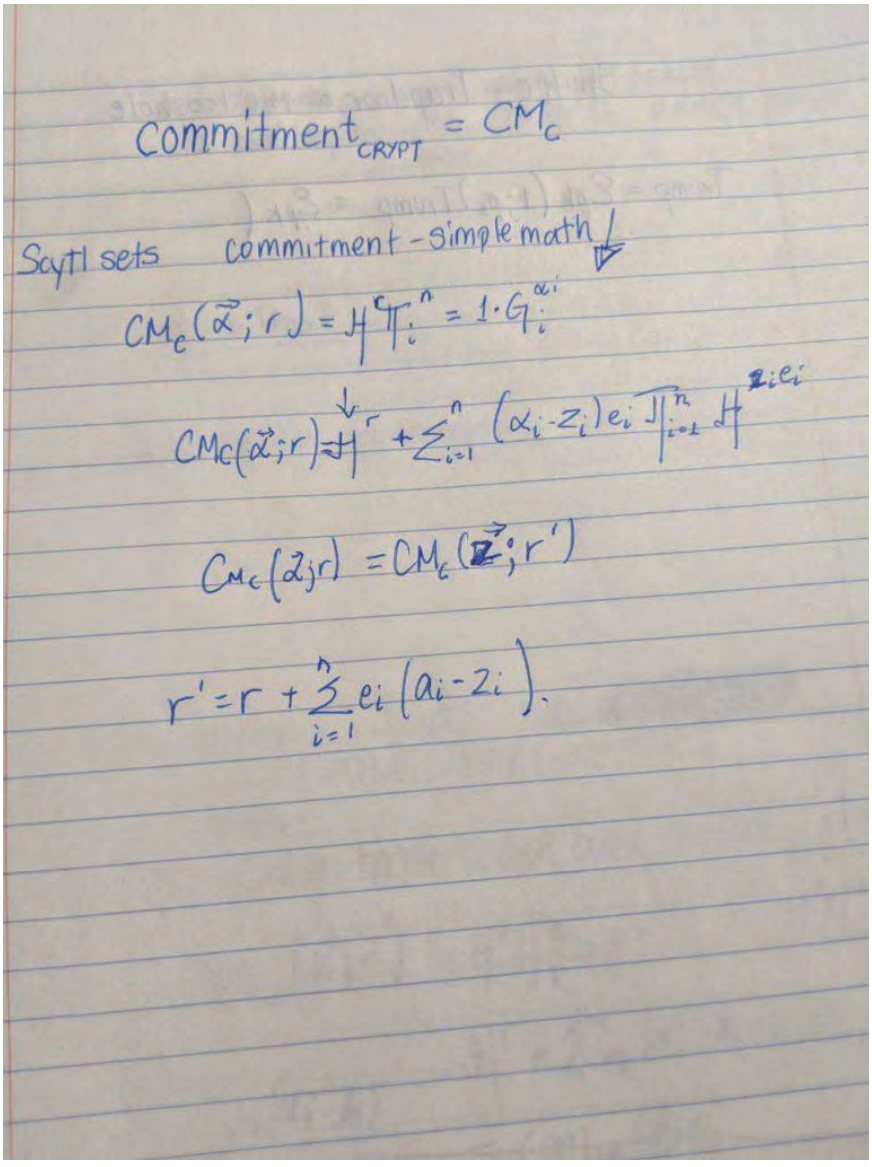
52. The encrypted data is shifted into Scytl's platform in the form of ciphertexts – this means it is encrypted and a key based on commitments is needed to read the data. The ballot data can only be read if the person has a key that is set on commitments.
53. A false sense of security is provided to 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."



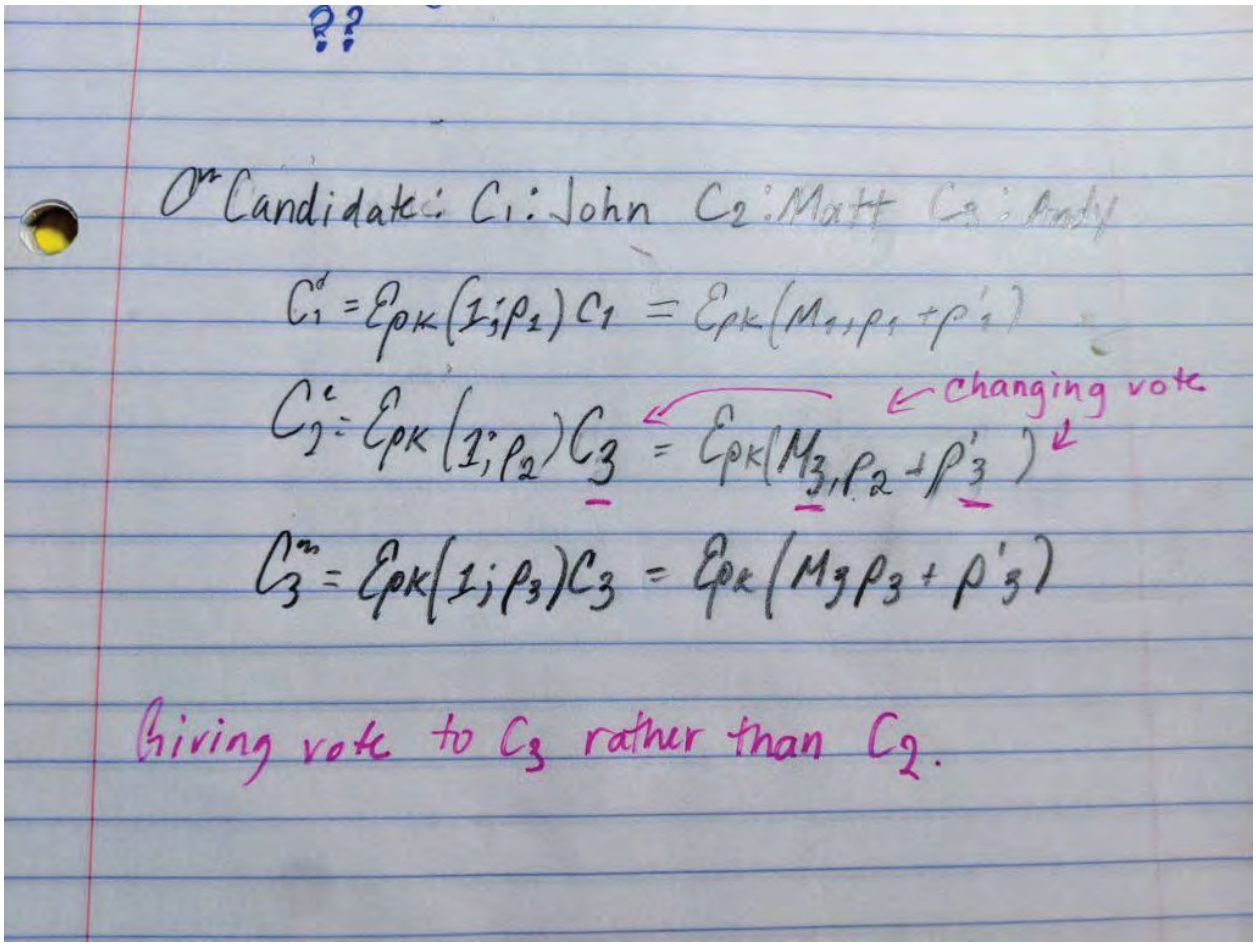
```
public CommitmentParams(final ZpSubgroup group, final int n) {
        group = group;
        h = GroupTools.getRandomElement(group);
        commitmentlength = n;
        g = GroupTools.getVectorRandomElement(group,
this.commitmentlength);
        }

        // 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)

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

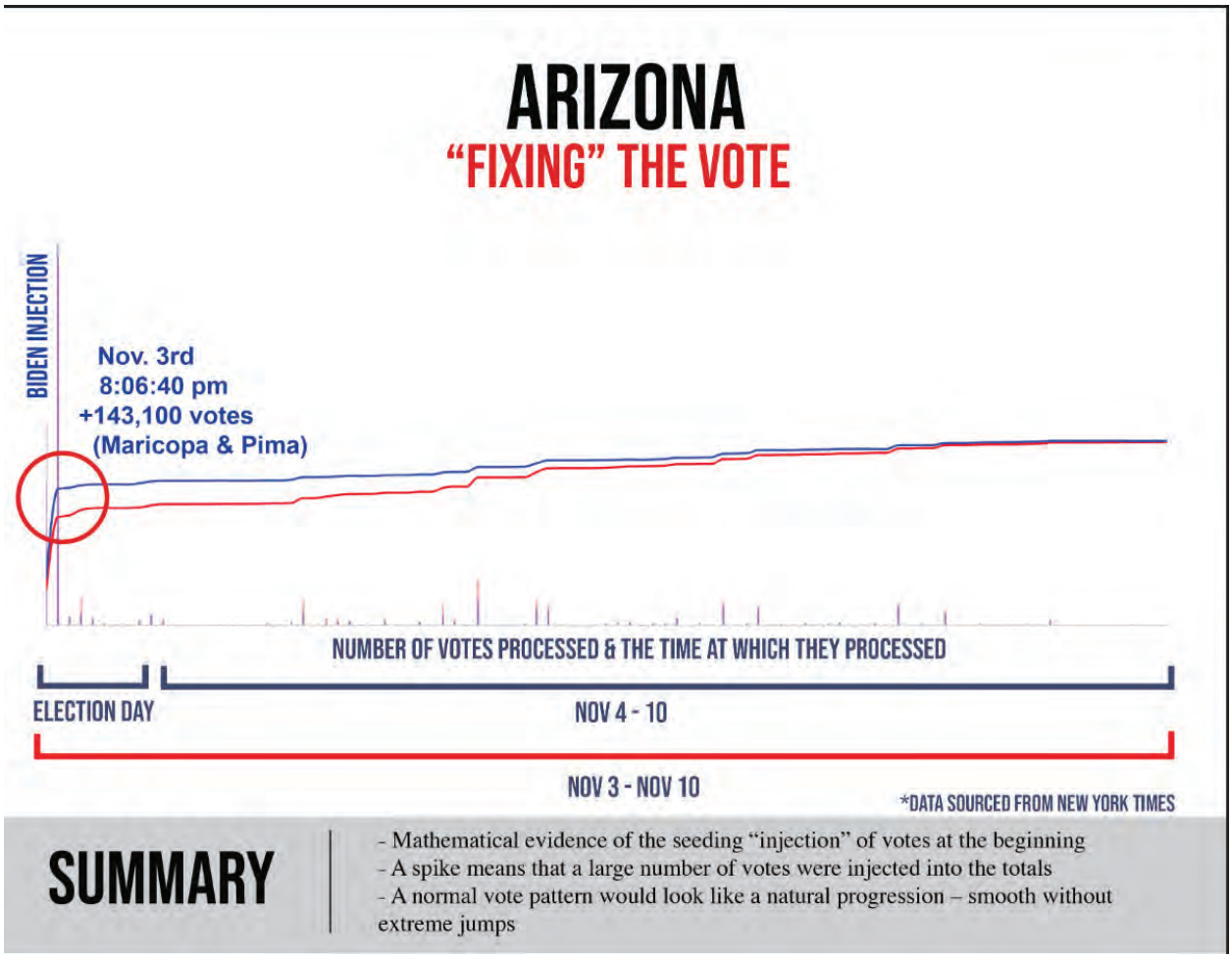
"reallocate" votes via an algorithm to achieve the goal set.



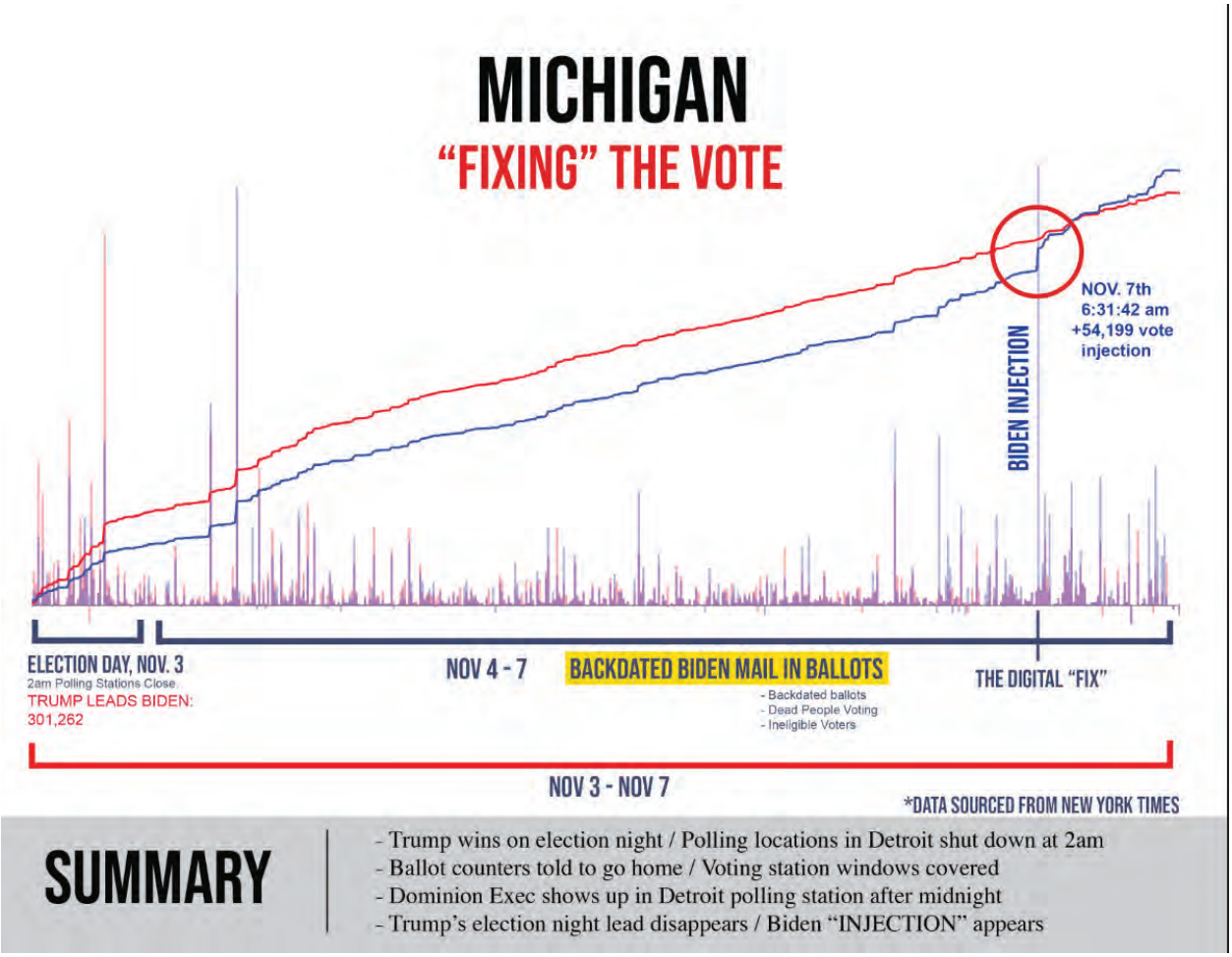
58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that 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 to 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.

69.


ARIZONA
"FIXING" THE VOTE
BIDEN INJECTION
Nov. 3rd
8:06:40 pm
+143,100 votes
(Maricopa & Pima)
NUMBER OF VOTES PROCESSED & THE TIME AT WHICH THEY PROCESSED
ELECTION DAY
NOV 4 - 10
NOV 3 - NOV 10
*DATA SOURCED FROM NEW YORK TIMES
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"

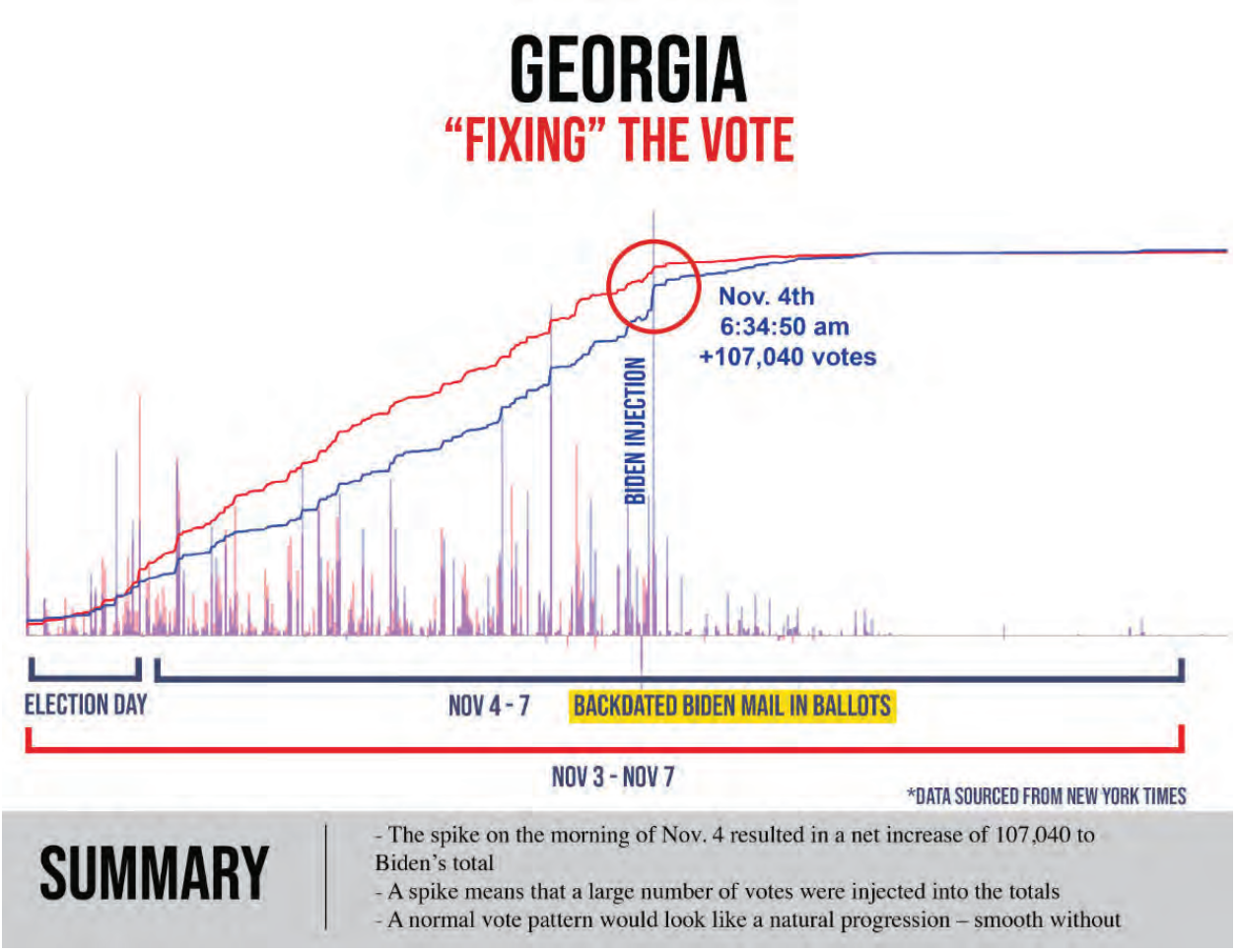
74. Observing the elections, after a review of Michigan's data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, 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.

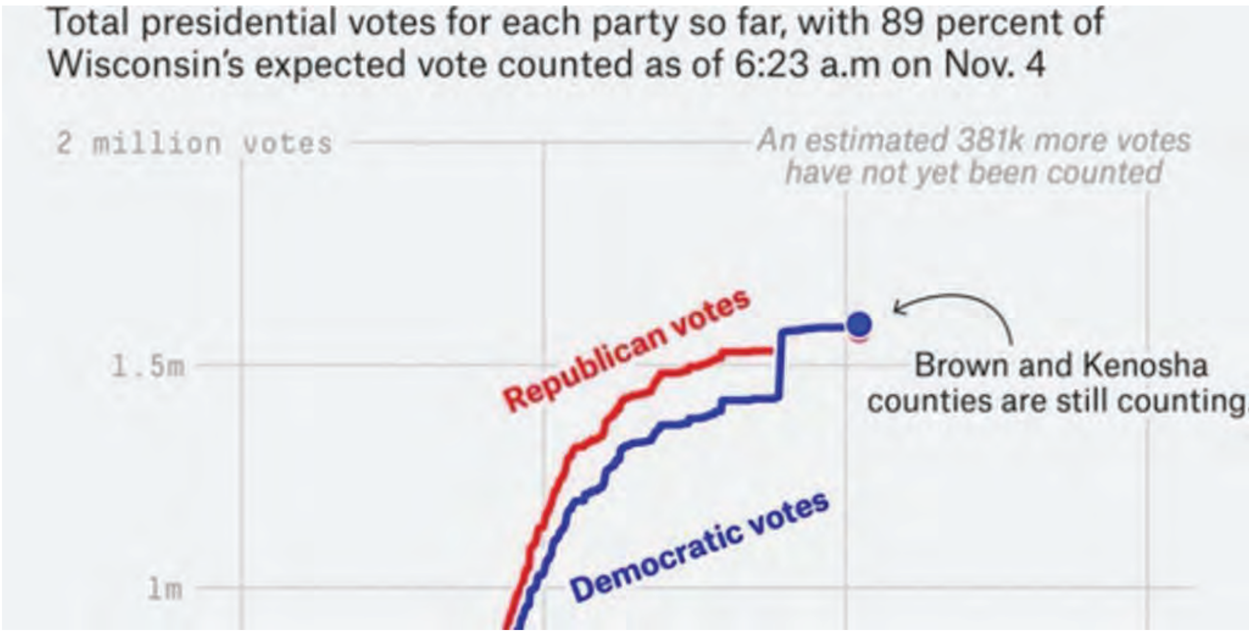
77. The algorithm looks to have been set to give Joe Biden a 52% win even with an initial 50K+ vote block allocation was provided initially as tallying began (as in case of Arizona too). In the am of November 4, 2020 the algorithm stopped working, therefore another "block allocation" to remedy the failure 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

the DHS servers was detected by the state of GA. The GA leadership assumed that it was "Russians" but later they found out that the IP address was that of DHS.

80. In the state of Wisconsin, we observed a considerable BLOCK vote allocation by the algorithm at the SAME TIME it happened across the nation. All systems shut down at around the same time.

81. 

82. In Wisconsin there are also irregularities in respect to BALLOT requests. (names AND address Hidden for privacy)

83.

F	G	H	V	W	X	Y	AB	AC	AD	AG	AH	AI	AJ	AK	AL
Active	Registered	Military	Brown County	11/01/2020	Online	Military		Official	Active	Not Returned	Online	11/01/2020			
Active	Registered	Regular	Brown County	10/23/2020	Voted In Person	Regular		Official	Active	Returned	Voted In Person	10/23/2020	10/23/2020		
Active	Registered	Military	Brown County	11/01/2020	Online	Military		Official	Active	Not Returned	Online	11/01/2020			
Active	Registered	Regular	Brown County	11/01/2020	Online										
Active	Registered	Regular	Brown County	11/01/2020	Email	Regular		Official	Active	Returned	Mail	10/31/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/01/2020	Email	Regular		Official	Active	Returned	Mail	10/31/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Voted In Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Voted In Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Voted In Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Voted In Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Voted In Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Online										
Active	Registered	Regular	Brown County	11/02/2020	Received In Person	Hospitaliz		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Email	Hospitaliz		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020		
Active	Registered	Military	Brown County	11/02/2020	Mail										
Active	Registered	Regular	Brown County	11/02/2020	Mail	Regular		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020		
Active	Registered	Regular	Brown County	11/02/2020	Mail	Regular		Official	Active	Returned	Appointed Agent		11/02/2020		
Active	Registered	Military	Brown County	11/02/2020	Online	Military		Official	Active	Not Returned	Online	11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	Online	Military		Official	Active	Not Returned	Online	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Online										
Active	Registered	Military	Brown County	11/02/2020	FPCA	Military		Official	Active	Not Returned	Mail	11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	FPCA	Military		Official	Active	Returned	Email	11/02/2020	11/03/2020		
Active	Registered	Regular	Brown County	11/03/2020	Voted In Person	Regular		Official	Inactive	Voter Spoiled	Voted In Person	11/03/2020	11/03/2020		
Active	Registered	Military	Brown County	11/03/2020	Mail	Military	Certification insufficient	Federal Absent	Active	Returned, to be Rejected	Mail	11/03/2020	11/03/2020		
Active	Registered	Military	Brown County	11/03/2020	Mail	Military		Official	Active	Not Returned	Mail	11/03/2020			
Active	Registered	Military	Brown County	11/03/2020	Online										
Active	Registered	Regular	Brown County	11/03/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										
Active	Registered	Regular	Brown County	11/04/2020	Online										

84.

Active	Registered	Regular	Brown County	11/03/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/06/2020	Online
Active	Registered	Regular	Brown County	11/06/2020	Online

85. I can personally attest that in 2013 discussions by the Obama / Biden administration were being had with various agencies in the deployment of such election software to be deployed in ----- in 2013.
86. On or about April 2013 a one year plan was set to fund and usher elections in -----.
87. Joe Biden was designated by Barack Hussein Obama to ensure the ----- accepted assistance.
88. John Owen Brennan and James (Jim) Clapper were responsible for the ushering of the intelligence surrounding the elections in -----.
89. Under the guise of Crisis support the US Federal Tax Payers funded the deployment of the election software and machines in ------ signing on with Scytl.

The White House

Office of the Press Secretary

For Immediate Release April 21, 2014

SHARE THIS: TWITTER FACEBOOK EMAIL

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.

90.

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 in 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.

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

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 Communique dated January 2009).

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

DEPARTMENT OF COMMERCE * UNITED STATES OF AMERICA *

For the National Voluntary Laboratory Accreditation Program

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	***SanDisk Ultra: SDCFHS-004G SDCFHS-008G RiData: CFC-14A RDF8G-233XMCB2-1 RDF16G-233XMCB2-1 RDF32G-233XMCB2-1 SanDisk Extreme: SDCFX-016G SDCFX-032G SanDisk: 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

NVLAP®

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

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.

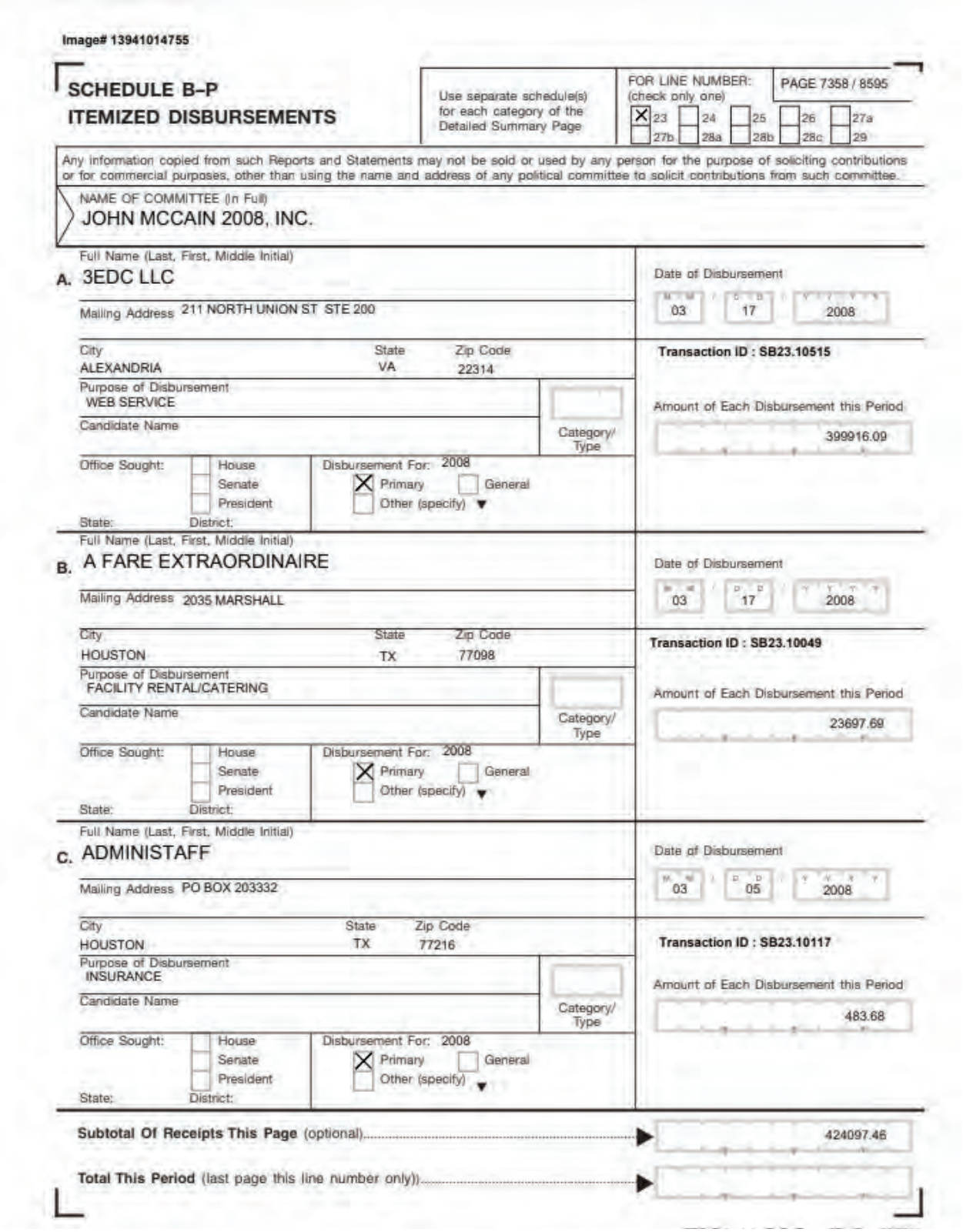
117. GEMS was manifested from SOE software purchased by SCYTL developers and US Federally Funded persons to develop it.

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.



Image# 13941014755

SCHEDULE B–P
ITEMIZED DISBURSEMENTS

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

FOR LINE NUMBER: (check only one)
☒ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27a
☐ 27b ☐ 28a ☐ 28b ☐ 28c ☐ 29

PAGE 7358 / 8595

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.

A. Full Name (Last, First, Middle Initial)
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
State: District:
Disbursement For: 2008 ☒ Primary ☐ General ☐ Other (specify)
Date of Disbursement 03 / 17 / 2008
Transaction ID : SB23.10515
Amount of Each Disbursement this Period 399916.09

B. Full Name (Last, First, Middle Initial)
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
State: District:
Disbursement For: 2008 ☒ Primary ☐ General ☐ Other (specify)
Date of Disbursement 03 / 17 / 2008
Transaction ID : SB23.10049
Amount of Each Disbursement this Period 23697.69

C. Full Name (Last, First, Middle Initial)
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
State: District:
Disbursement For: 2008 ☒ Primary ☐ General ☐ Other (specify)
Date of Disbursement 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.

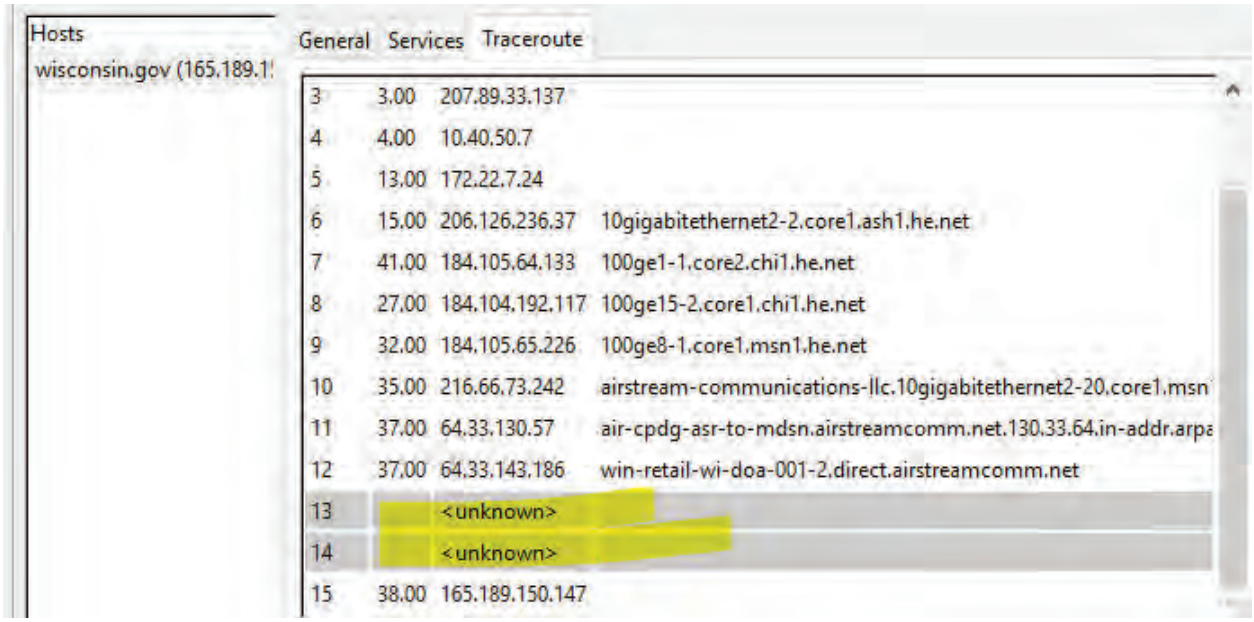
125. AKAMAI Technologies Houses ALL foreign government sites. (Please see White Paper by Akamai.)

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.

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.

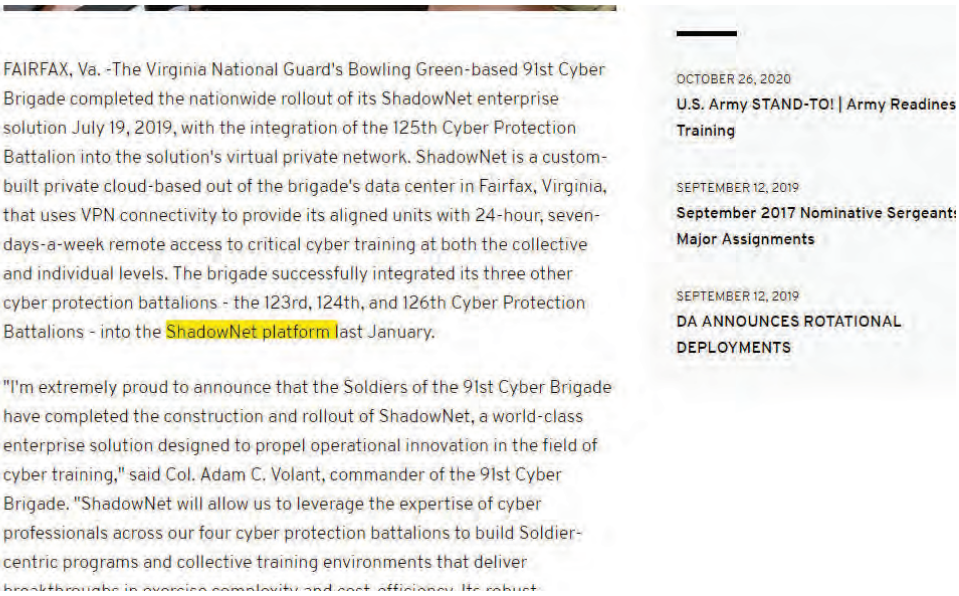
150. For the people of the United States to have confidence in their elections our cybersecurity standards should not be in the hands of foreign nations.

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 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 Readines
Training

SEPTEMBER 12, 2019
September 2017 Nominative Sergeants
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.

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	

155.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge.
Executed this November 29th, 2020.