

# Utah Voting System Manufacturer (VSM)

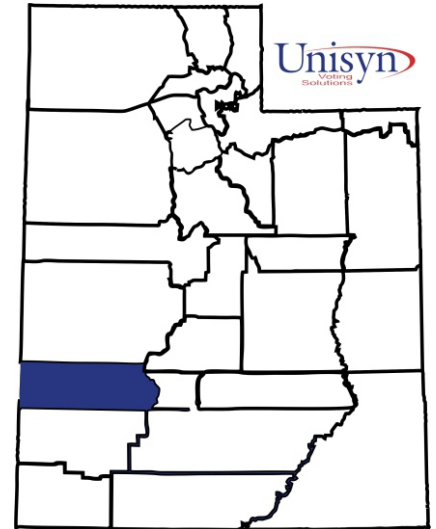
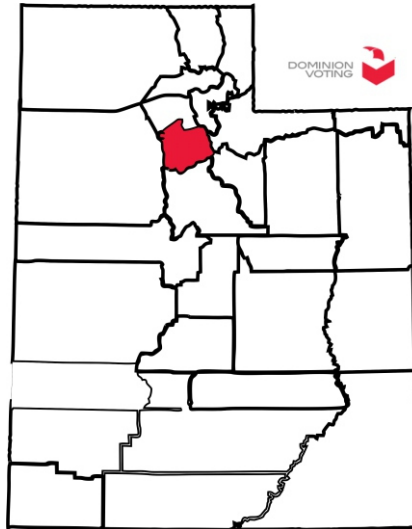
E&S is used by 27 Utah counties.

Dominion used by Salt Lake county

Unisyn used by Beaver county

2 not using ES&S are Salt Lake and Beaver

Diebold Assure 1.3  
ACCUVOTE TSx



## ES&S Election Voting System

(varies by county)

DS450 Scanner/Tabulator

- Steel Table/Cart
- Reports Printer
- Audit Printer
- Battery Backup
- USB Cables
- 8GB Thumb Drive

DS200 Scanner Tabulator

- Battery Backup
- Plastic Ballot Box w/steel door and e-bin
- Paper Roll
- 4GB Jump Drive
- EXV Power Supply Level VI 1

Election Management Hardware

- Dell Optiplex 5050 Mini Desktop Workstation OR Dell Optiplex 5040 Mini Desktop Workstation
- Symantec Endpoint Protection
- Adobe Acrobat Standard XI
- Uninterruptable Power Supply (UPS)
- OKI B432 Mono Laser Duplex Printer
- Startech 6' USB Cable
- ElectionWare Reporting Software
- Central Point Software
- Client/Server Election Management System

Other

- Evolution Printers w/firmware
- MBV 1000
- Third Party EMS Hardware
- DS2 4GB Thumb Drive
- 2GB Thumb Drive
- Counting DBS-Elections and Election Supplies
- Election Coding & Election Software/VoteByMail
- D-Link Router Gigabit 8port BOD Laptop
- CAT 5 10' Cable 25138

## Dominion Voting System

The information below is the safe diebold/ dominion version upgrades that we purchased in 2012 and installed in 2013. They only thing that we installed since then was a new certificate that allowed us to keep using the software/firmware.

Information:

**Touchscreen**

- Diebold AVTSX Build Number 4.7.10

**Ballot Scanner**

- Photocrite PS900 v2.6.2

**Tabulation Software**

- Dominion Voting Systems GEMS v1.21.6.0
- Premier Election Systems PCS v2.2.5.0

**Electronic Poll Books Hardware**

- Apple iPad (6th Generation)

**Electronic Poll Books Software**

- KNOWINK PollPad3 v2.5.0

Thank you,

Lannie



Lannie K. Chapman  
Chief Deputy Clerk  
Salt Lake County Clerk  
[LKChapman@slco.org](mailto:LKChapman@slco.org)  
385-468-7420

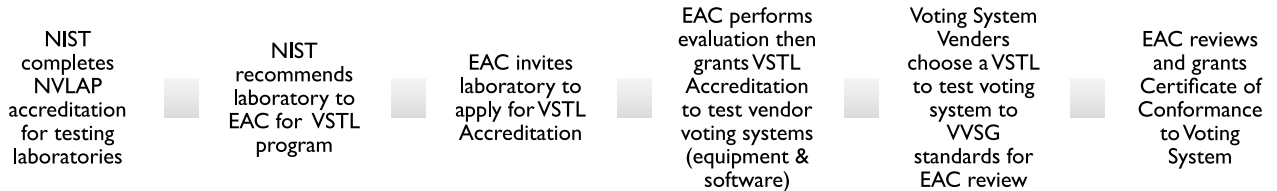
[SLCO Clerk Website](http://slco.org)

## Unisyn Voting System

- OVCS OpenElect 2..0
  - OVSCmini bulk ballot scanner (no PC)
  - Ballot Optical Scanner
  - Touchscreen ADA
  - Voting Central Scan Mini
  - Locking Ballot Box w/lid
  - Laptop Server Computer

Information from GRAMA submitted to all Utah Counties.  
Information is only as accurate as documents provided by those counting.

# EAC Voting Equipment Certification Process



## Elections Assistance Commission

*(EAC) created by HAVA 2002*

- Testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories
  - Voting equipment system Certificate of Compliance to VVSG by VSTL
  - Voluntary System Test Lab (VSTL) accreditation
    - Re-accreditation every 2 years
    - NIST certification and recommendation (optional)
      - NVLAP accreditation

- Develop guidance to meet HAVA requirements
- National Clearinghouse
  - resource for compilation of information on election administration
- Promote effective administration of Federal elections
- Manage HAVA Grants
  - Provide information and training
  - Management of grant payments
- Adopt Voluntary Voting System Guidelines (VVSG)

### • 4 Commissioners

- Nominated by the President and confirmed by Senate to serve 4 year term or to finish term of vacant position
- Current Commissioners
  - Donald Palmer, Chair
  - Thomas Hicks, Vice Chair
  - Christy McCormick
  - Benjamin Hovland

### • EAC Directors:

- Executive Director, Mona Harrington
- General Counsel, Kevin Rayburn
- Testing & Certification Director, Jerome Lovato
- Research Director, Nichelle Williams
- Communications Director, Kristen Muthig
- Financial Director, Paul Repak

### • 3 Boards:

- Standards Board
- Board of Advisors
- Technical Guidelines Development Committee (TGDC)

# How does EAC accredit VSTL



## EAC Testing & Certification Director

- 1) Notifies laboratory of Commissioners' decision
- 2) Issues Certificate of Accreditation
- 3) Makes VSTL information "available to public on EAC's Website"

3.6.1. Certificate of Accreditation. A Certificate of Accreditation shall be issued to each laboratory accredited by vote of the Commissioners. The certificate shall be signed by the Chair of the Commission and state:

3.6.1.1. The name of the VSTL;

3.6.1.2. The scope of accreditation, by stating the Federal standard or standards to which the VSTL is competent to test;

3.6.1.3. The effective date of the certification, which shall not exceed a period of two (2) years; and

3.6.1.4. The technical standards to which the laboratory was accredited.

3.7. **Effect of Accreditation.** Receipt of an EAC Accreditation indicates that a laboratory has met the applicable technical, procedural, management and staffing requirements and may serve as a Voting System Test Laboratory (VSTL) under EAC's Testing and Certification Program.

3.7.1. Scope of Accreditation. A laboratory shall operate within the limits of the scope of accreditation as stated on its Certificate of Accreditation.

3.7.2. Representation. No VSTL may make representations regarding its accreditation beyond its scope of accreditation.

3.7.3. No Endorsement. A Certificate of Accreditation is **not** an endorsement of the recipient laboratory. A VSTL may not state or imply EAC endorsement.

3.8. **Expiration and Renewal of Accreditation.** A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation. VSTLs in good standing shall renew their accreditation by submitting an application package to the Program Director, consistent with the procedures of Section 3.4 of this Chapter, no earlier than 60 days before the accreditation expiration date and no later than 30 days before that date. Laboratories that timely file the renewal application package shall retain their accreditation while the review and processing of their application is pending. VSTLs in good standing shall also retain their accreditation should circumstances leave the EAC without a quorum to conduct the vote required under Section 3.5.5.

3.6.2. Post Information on Web Site. The Program Director shall make information pertaining to each accredited laboratory available to the public on EAC’s Web site. This information shall include (but is not limited to):

- 3.6.2.1. NIST’s Recommendation Letter;
- 3.6.2.2. The VSTL’s Letter of Agreement;
- 3.6.2.3. The VSTL’s Certification of Conditions and Practices;
- 3.6.2.4. The Commissioner’s Decision on Accreditation; and
- 3.6.2.5. The Certificate of Accreditation.

### Letter to Pro V&V dated Sep 27, 2012 regarding EAC VSTL accreditation

- Lack of Quorum of Commissioners to vote
- VSTL cannot be accredited without a vote of the commissioners
- VSTL accreditation must wait until quorum of Commissioners “have been appointed, approved, and received their Commissions”

On August 2, 2012, EAC Acting Executive Director and COO Alice Miller received a letter from National Institute of Standards and Technology (NIST) Director Patrick Gallagher stating that NIST had completed its comprehensive technical evaluation of laboratory competence to test voting systems to the EAC 2005 Voluntary Voting System Guidelines (VVSG). Director Gallagher also proposed that Pro V&V be accredited by the EAC under the provisions of the Help America Vote Act of 2002 (HAVA).

In addition, on April 9, 2012, the EAC received responses from Pro V&V adequately addressing three nonconformities and two comments noted during the EAC laboratory audit of Pro V&V conducted on February 24, 2012 and noted in our Voting System Test Laboratory Initial Assessment Report dated March 21, 2012.

At this point Pro V&V has met all procedural requirements of both NIST and the EAC Voting System Test Laboratory Program in order to be accredited as an EAC Voting System Test Laboratory (VSTL). The last component of VSTL accreditation is a positive vote by EAC Commissioners as required by Section 231(b)(2) of HAVA. Because the EAC currently lacks a quorum of Commissioners to vote on your accreditation, the EAC will hold all documentation in readiness and present your material for a vote by EAC Commissioners at the earliest opportunity after a quorum of Commissioners have been appointed, approved and received their Commissions.

### Where is:

1. VSTL Name
2. Scope of Accreditation by federal standards
3. Technical Standards of Accreditation
4. Effective Start Date of Certificate
5. Effective End Date of Certificate  
“shall not exceed a period of 2 years”
6. Signed by the Chair of the Commission  
Feb 2015 to Feb 2016 Christy McCormick served as Chair of EAC



Expired When?

OOPS, signed by Acting Executive Director

## Where is:

1. VSTL Name
2. Scope of Accreditation by federal standards
3. Technical Standards of Accreditation
4. Effective Start Date of Certificate
5. Effective End Date of Certificate  
"shall not exceed a period of 2 years"
6. Signed by the Chair of the Commission  
Feb 2017 to Feb 2018 Matthew Materson served as Chair of EAC



Expired When?

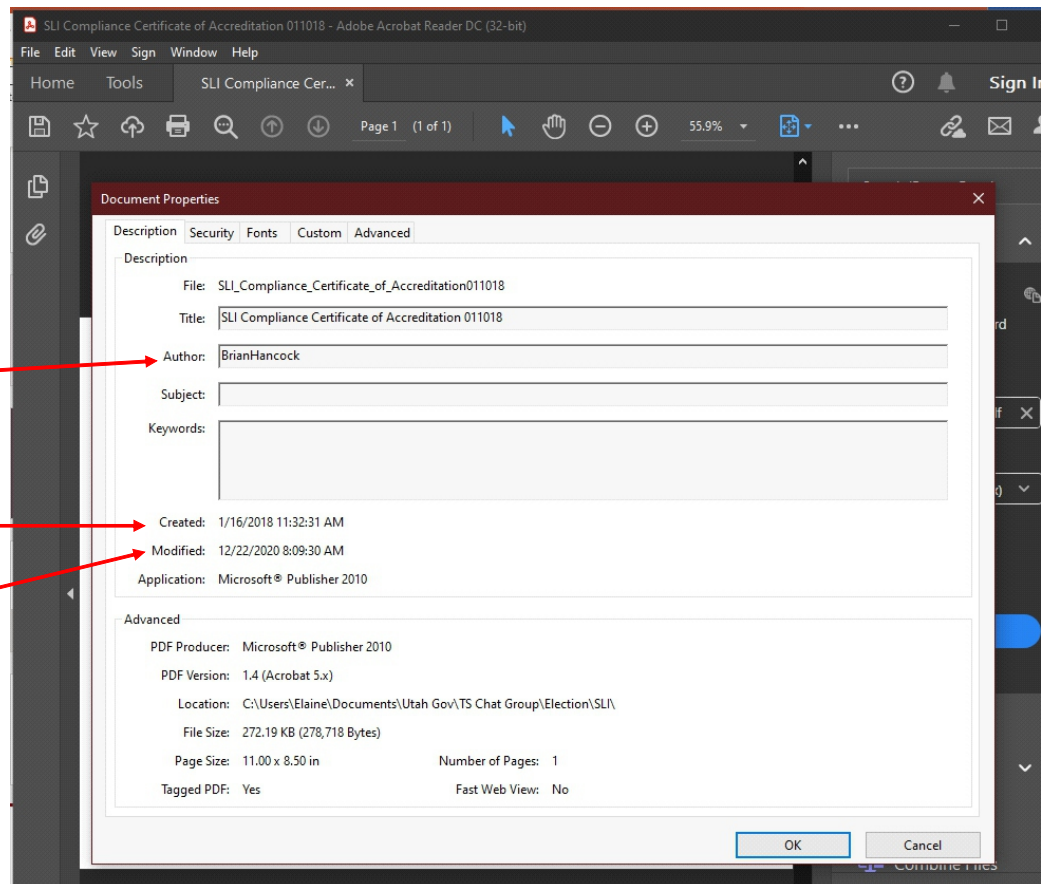
OOPS, signed by Executive Director

## Closer Look at Document Properties

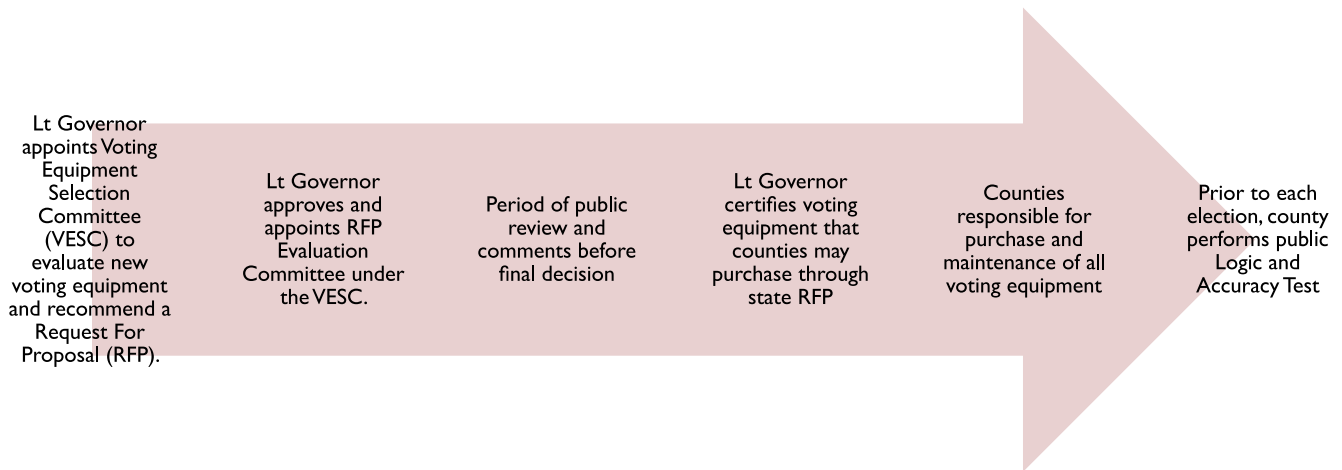
Testing & Certification Director, Brian Hancock retired from EAC 28 Feb 2019

Created 16 Jan 2018

Modified 22 Dec 2020



# Utah Voting Equipment Certification



[C20A-5-P8\\_2017050920170509.pdf \(utah.gov\)](#)



## Utah uses EAC certified voting systems that are tested by EAC accredited Voting System Test Labs (VSTL).

### Utah Code 20A-5-802

- (2) (a) Except as provided in Subsection (2)(b)(ii):
- (i) the lieutenant governor shall ensure that all voting equipment used in the state is independently tested using security testing protocols and standards that:
    - (A) are generally accepted in the industry at the time the lieutenant governor reviews the voting equipment for certification; and
    - (B) meet the requirements of Subsection (2)(a)(ii);
  - (ii) the testing protocols and standards described in Subsection (2)(a)(i) shall require that a voting system:
    - (A) is accurate and reliable;
    - (B) possesses established and maintained access controls;
    - (C) has not been fraudulently manipulated or tampered with;
    - (D) is able to identify fraudulent or erroneous changes to the voting equipment; and
    - (E) protects the secrecy of a voter's ballot; and
  - (iii) The lieutenant governor may comply with the requirements of Subsection (2)(a) by certifying voting equipment that has been certified by:
    - (A) the United States Election Assistance Commission; or
    - (B) a laboratory that has been accredited by the United States Election Assistance Commission to test voting equipment.
- (b) (i) Voting equipment used in the state may include technology that allows for ranked-choice voting.
- (ii) The lieutenant governor may, for voting equipment used for ranked-choice voting under Title 20A, Chapter 4, Part 6, Municipal Alternate Voting Methods Pilot Project, certify voting equipment that has been successfully used within the United States or a territory of the United States for ranked-choice voting for a race for federal office.

Amended by Chapter 305, 2019 General Session

According to email received from a GRAMA request, all Utah counties with ES&S voting systems received an upgrade to EVS 6.0.4.0 in Summer/Fall of 2019

**United States Election Assistance Commission**

---

**Certificate of Conformance**

---

**ES&S EVS 6.0.4.0**

The voting system identified on this certificate has been evaluated at an accredited voting system testing laboratory for conformance to the *Voluntary Voting System Guidelines Version 1.0 (VVSG 1.0)*. Components evaluated for this certification are detailed in the attached Scope of Certification document. This certificate applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been verified by the EAC in accordance with the provisions of the *EAC Voting System Testing and Certification Program Manual* and the conclusions of the testing laboratory in the test report are consistent with the evidence adduced. This certificate is not an endorsement of the product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.


Product Name: EVS

Model or Version: 6.0.4.0

Name of VSTL: SLI Compliance

EAC Certification Number: ESSEVS6040

Date Issued: May 3, 2019

  
\_\_\_\_\_  
*Executive Director*

**Scope of Certification Attached**

**United States Election Assistance Commission**

---

**Certificate of Conformance**

---

**OpenElect 2.0.A.2**

The voting system identified on this certificate has been evaluated at an accredited voting system testing laboratory for conformance to the 2005 *Voluntary Voting System Guidelines (2005 VVSG)*. Components evaluated for this certification are detailed in the attached Scope of Certification document. This certificate applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been verified by the EAC in accordance with the provisions of the *EAC Voting System Testing and Certification Program Manual* and the conclusions of the testing laboratory in the test report are consistent with the evidence adduced. This certificate is not an endorsement of the product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

Product Name: OpenElect

Model or Version: 2.0.A.2

Name of VSTL: SLI Compliance

EAC Certification Number: UNS10121966-2.0.A.2

Date Issued: December 11, 2018

  
\_\_\_\_\_  
*Executive Director*  
*U.S. Election Assistance Commission*

**Scope of Certification Attached**



United States Election Assistance Commission



Certificate of Conformance

DVS Assure 1.3

The voting system identified on this certificate has been evaluated at an accredited voting system testing laboratory for conformance to the 2002 Voting System Standards (2002 VSS). Components evaluated for this certification are detailed in the attached Scope of Certification document. This certificate applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been verified by the EAC in accordance with the provisions of the EAC Voting System Testing and Certification Program Manual and the conclusions of the testing laboratory in the test report are consistent with the evidence adduced. This certificate is not an endorsement of the product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

Product Name: Dominion Assure
Model or Version: Version 1.3
Name of VSTL: SLI Global Solutions
EAC Certification Number: DVS-Assure1.3
Date Issued: June 29, 2012

Handwritten signature of J. P. Keller

Chief Operating Officer and Acting Executive Director
U.S. Election Assistance Commission

Scope of Certification Attached

Letter Report

PRO V&V



To: The Election Administration Resource Center dba Ranked Choice Voting Resource Center
From: Wendy Owens - Pro V&V, Inc.
CC: Keith Long - RCVRC; Alan Simmons, Michael Walker - Pro V&V, Inc.
Date: August 30, 2019
Subject: Universal RCV Tabulator v1.0.1

Dear RCVRC:

Pro V&V, a VSTL, is providing this letter to report the results of the modification testing performed on the RCVRC's Ranked Choice Voting Tabulator (Universal RCV Tabulator 1.0.1), a post-EMS secondary tabulator, which in this instance is an external software modification-addition to the ES&S's EVS 6.0.4.0 EAC Certified Voting System (ESSEVS6040 - May 03, 2019).

This testing campaign was performed, with the support of ES&S, to verify that the submitted modification-addition meets the certification requirements found in the Voluntary Voting System Guidelines Version 1.0 (VVSG 1.0).

To start, Pro V&V determined that this modification was subject only to limited certification testing as RCVRS was able to establish that this detached modification-addition did not affect the previously demonstrated compliance of the baseline system to the VVSG 1.0. Limited testing, in addition to other stated uses, is intended to facilitate the integration of vote counting software with other systems and election software. The following modifications to the previously certified system were evaluated:

- Addition of the Universal RCV Tabulator



STATE OF UTAH  
OFFICE OF THE LIEUTENANT GOVERNOR



SPENCER J. COX  
LIEUTENANT GOVERNOR

December 30, 2019

Susan Parmer  
Election Systems & Software, LLC  
11208 John Galt Blvd.  
Omaha, NE 68137

Dear Susan Parmer:

The Office of the Utah Lieutenant Governor reviewed engineering change order (ECO) #1043 and determined it has met the criteria of Utah Code § 20A-5-802. It is therefore approved. If you have any questions, please contact Derek Brenchley at 801-538-1041.

Sincerely,

Spencer J. Cox  
Utah Lieutenant Governor

October 8, 2019

Susan Parmer  
Election Systems & Software, LLC  
11208 John Galt Blvd.  
Omaha, NE 68137

Dear Ms. Parmer:

The Office of the Utah Lieutenant Governor reviewed the voting equipment certification application for the Universal RCV Tabulator v1.0.1. Pro V&V, a laboratory that has been accredited by the United States Election Assistance Commission (EAC), determined that the Universal RCV Tabulator v1.0.1 meets the required acceptance criteria of the EAC Voluntary Voting System Guidelines (Version 1.0).

The testing results from Pro V&V meet the voting equipment certification requirements outlined by Utah Code Annotated § 20A-5-802; therefore, the Universal RCV Tabulator v1.0.1 is certified by the State of Utah.

Sincerely,

Spencer J. Cox  
Utah Lieutenant Governor

June 9, 2020

Susan Parmer  
Election Systems & Software, LLC  
11208 John Galt Blvd.  
Omaha, NE 68137

Dear Ms. Parmer:

The Office of the Utah Lieutenant Governor reviewed engineering change order (ECO) #1068 and determined it has met the criteria of Utah Code § 20A-5-802. It is therefore approved for use in Utah. Please contact Derek Brenchley at 801-538-1746 if you have any questions.

Sincerely,

Spencer J. Cox  
Utah Lieutenant Governor

October 8, 2019

Susan Parmer  
Election Systems & Software, LLC  
11208 John Galt Blvd.  
Omaha, NE 68137

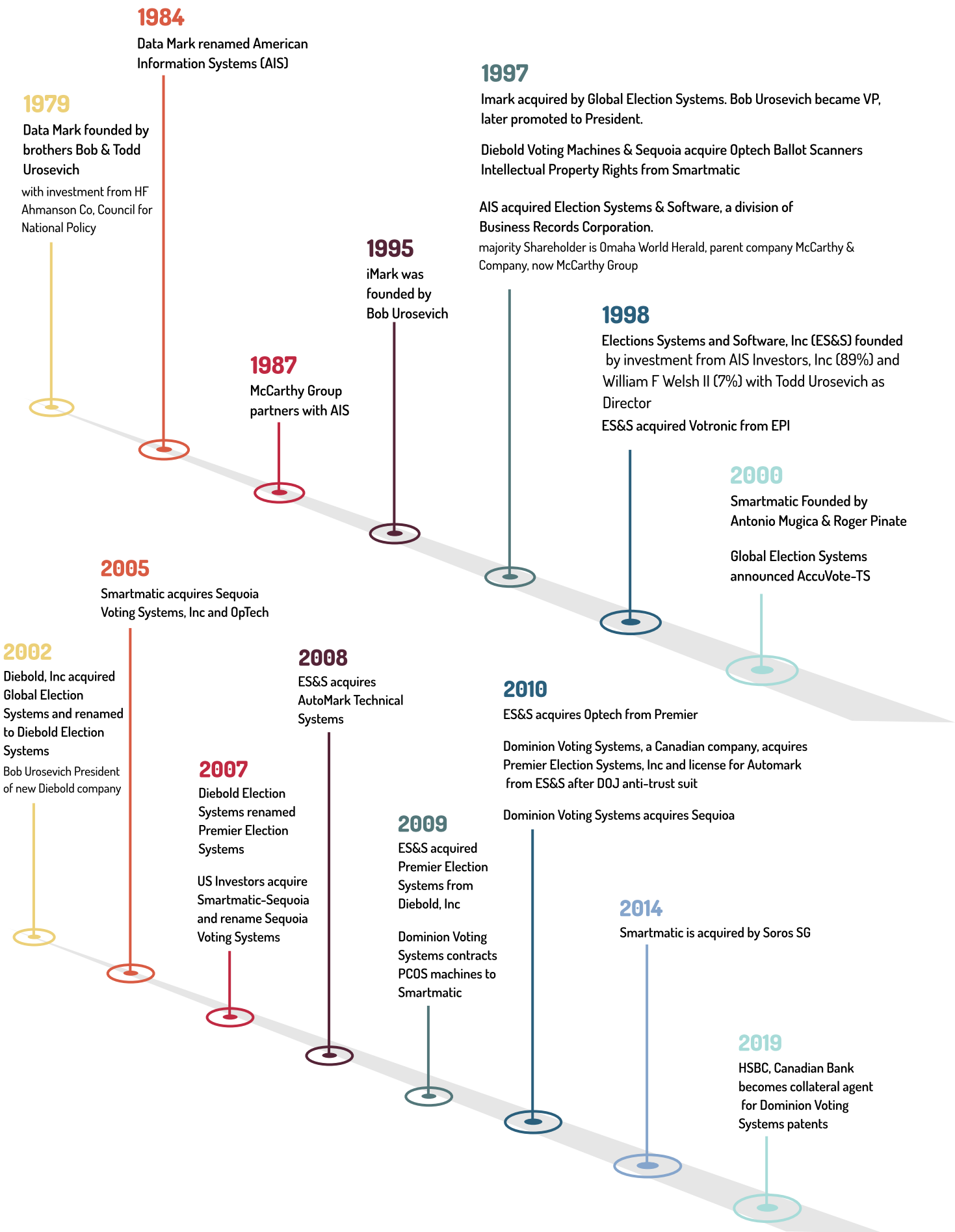
Dear Ms. Parmer:

The Office of the Utah Lieutenant Governor reviewed the voting equipment certification application for the Universal RCV Tabulator v1.0.1. Pro V&V, a laboratory that has been accredited by the United States Election Assistance Commission (EAC), determined that the Universal RCV Tabulator v1.0.1 meets the required acceptance criteria of the EAC Voluntary Voting System Guidelines (Version 1.0).

The testing results from Pro V&V meet the voting equipment certification requirements outlined by Utah Code Annotated § 20A-5-802; therefore, the Universal RCV Tabulator v1.0.1 is certified by the State of Utah.

Sincerely,

Spencer J. Cox  
Utah Lieutenant Governor



# Voting System Manufacturers All Use the Same Software



**American  
Information  
Systems (AIS)**



## Company Acquisitions

DataMark ▶ AIS ▶ ES&S

Sequoia ▶ Diebold ▶ Smartmatic-Sequoia ▶ Sequoia Voting Systems ▶ Dominion

Diebold/Premier ▶ ES&S ▶ Dominion

## Software Licensing and/or Acquisition

OpTech ▶ Diebold ▶ Smartmatic ▶ Sequoia ▶ Dominion ▶ ES&S

AutoMark Diebold ▶ ES&S ▶ Dominion

GEMS ▶ Smartmatic ▶ Diebold ▶ ES&S ▶ Dominion

## Sources

Accesswire. (2017). *Voting Technology Companies in the US--Their Histories and Present Conditions*.

Alaska SOS Business entity search: Elections Systems & Software

Blumenthal, D. (2020). *Dominion Voting Patents To China Bank (HSBC) for Collateral..*

Cohn, J. (2017). *Voting Machine Company Mega Thread Part 1-203 sourced posts*.  
<https://www.protectourvotes.com/wp->

Court of Chancery of the State of Delaware. (2008). *Smartmatic Corp v. SVS Holdings, Inc and Sequoia Voting*

Friedman, B. (2010). *On Heals of Diebold/Premier Purchase, Canadian eVoting Firm Dominion Also Acquires*

Fitrakis, B and Wasserman, H.. (2004). *Diebold's Political Machine*. <https://www.motherjones.com/politics/2004/03/diebolds-political-machine/>

Huseman, J. (2019). *The Market for Voting Machines Is Broken. This Company Has Thrived in It*. ProPublica.

Nebraska SOS Business entity search: Election Systems & Software & American Information Systems

Omaha World Herald. (2008). *The Omaha World-Herald's Share of ES&S*. <http://contantinereport.com/the-omaha-heralds-share-of-ess/>.

Online Image (2020). *GEMS Software is KEY*. <https://pbs.twimg.com/media/EnSAJapWMAQtyce.jpg>

Pedrosa, C. (2012). *Damning evidence against Smartmatic PCOS*. Philstar Global. <https://www.philstar.com/opinion/2012/11/10/864977/damning-evidence-against-smartmatic-pcos>.

USPTO. (2021). *Patent Assignment Search: 050500/0236*. <https://assignment.uspto.gov/patent/index.html#/patent/search/resultAssignment?id=50500-236>.



# Foreign Interference In Elections

Link to Dominion Voting System Patents to China

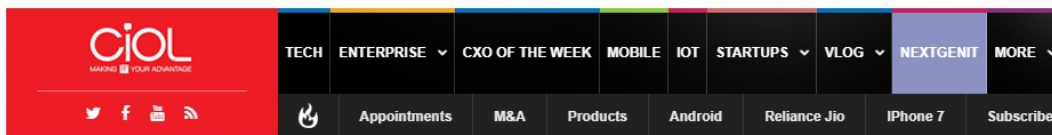
<https://assignment.uspto.gov/patent/index.html#/patent/search/resultAssignment?id=50500-236>  
<https://drdannielleblumenthal.wordpress.com/2020/11/25/dominion-voting-patents-to-china-bank-hsbc-for-collateral/>

Link to Col. Waldron, “Your Wake Up Call” documentary that goes into foreign interference.

<https://cdn.frankspeech.com/YourWakeUpCallFinalWeb11m4v196947/mp4/YourWakeUpCallFinalWeb11m4v196947.mp4>

Scytl election reporting

<https://www.commdiginews.com/politics-2/swiss-and-aussies-find-a-critical-flaw-in-scytl-software-that-the-us-ignores-134093/>



## Scytl continues leading election modernization industry

ENTERPRISE By : | September 23, 2013

**B**ARCELONA, SPAIN & TAMPA, USA: Scytl, the worldwide leader in secure online voting and election modernization, continues receiving electoral and industry expert recognition for its end-to-end election modernization technology and electoral roadmap implementation approach from organizations such as IDC, Ovum and ACEEEO.

Scytl’s end-to-end election modernization solution covers the full election cycle (Pre-election, Election Day and Post-election), providing electoral bodies the most secure, transparent, auditable and accessible solution in the marketplace and allows Scytl to offer personalized election modernization roadmaps to their customers combining both traditional and online voting solutions as needed.

### *Election modernization views from leading industry experts*

**IDC** – In the recently published IDC Government Insights “Technology Spotlight: Delivering End-to-End Election Modernization Roadmaps” sponsored by Scytl, leading analyst firm IDC highlights Scytl’s value proposition and benefits: a comprehensive solution for the entire election process, the ability to deliver specific election modernization roadmaps for individual electoral bodies enabling an “evolve as you need” approach, in depth and specific experience in providing online voting capabilities (18 out of 20 countries that have implemented online binding public elections) and a full range of security options.

**Ovum** – Scytl’s background, experience and penetration in online voting based on a strong security framework ensures not only leading edge functionality and tailoring required for different election processes in different regions, but also end-to-end security, distinguishing it from other vendors on the market.

In 2014, Smartmatic CEO Antonio Mugica and British Lord Mark Malloch-Brown announced the launching of the SGO Corporation Limited



Doug Emhoff took a leave of absence from the law firm, [DLA Piper](#), in August, after now President-elect [Joe Biden](#), a Democrat, named Harris as his running mate. A Biden campaign representative said Emhoff will sever all ties with [DLA Piper](#) by Inauguration Day, Jan. 20, 2021.



Sir Nigel Knowles is the former global co-chairman of the law firm [DLA Piper](#) & Current Director at [SGO Corp Ltd](#)



Antonio Mugica founder and CEO of Smartmatic



Corp Ltd London UK



Lord Mark Malloch Brown, The Soros Open Society Foundation co-founder & board Member, owns [Smartmatic \(Dominion Voting Systems\)](#)



**Kamala Harris's Husband ????**  
**Connections To Smartmatic & Dominion Voting Systems...**  
 BY CLOVERCHRONICLE ON NOVEMBER 16, 2020

- <https://cloverchronicle.com/2020/11/15/kamala-harriss-husband-douglas-emhoff-may-have-connections-to-smartmatic-dominion-voting-systems/>
- <https://www.biometricupdate.com/201411/smartmatic-spins-off-new-parent-company-sgo-with-british-lord>
- <https://economictimes.indiatimes.com/news/international/world-news/vice-president-elect-kamala-harris-husband-leaves-job-at-powerhouse-law-firm-dla-piper/articleshow/79163865.cms>

# HUAWEI TENTACLES IN EASTERN EUROPE

Roaming Networks, a relatively unknown corporation based in Serbia run by oligarch **Nenad Kovac**<sup>1</sup>, was selected as the enterprise partner of Huawei (CCP) to install their technology into eastern Europe.<sup>2</sup> Roaming Networks ...

- 1) Installed Huawei radio communications equipment in Serbia for multiple telecom corporations;
- 2) Worked with T-Mobile in Austria to install Huawei equipment for 3600 cell towers; and
- 3) Built a large CCTV system in Belgrade for a “safe city project” using *turnkey* Huawei FTTx network equipment. Denmark’s TDC Telecom also received a Huawei injection. Roaming enabled CCP-owned Huawei to run the Serbian nationwide transport network, including railways, electric power, and wind. Roaming built their own HQ data center using Huawei tech, and was rewarded with the *design, implementation, and 24x7 maintenance* of the Bank of China. Even the National Assembly of Serbia is now wired with Huawei. In 2017, they lost their license to operate in Denmark.<sup>3</sup>

**ICT INFRASTRUCTURE AND DATA CENTER**

**Telekom Srbija**

**Huawei, Infinera, Nokia:**

- MiniPAN/MSAN/DSLAM installation of access equipment nationwide
- Installation and commissioning of DWDM equipment for nationwide transport network
- Technical support for maintenance of DWDM equipment

**EPS (Electric Power Industry of Serbia)**

**Huawei:**

- Delivery installation and implementation of DWDM equipment for nationwide transport network
- 24/7 Managed service of monitoring and maintenance of DWDM transport network
- Technical support for maintenance of DWDM transport network

**Nokia:**

- Technical support for maintenance of SDH transport network

**Elektro mreža Srbije (Serbian transmission system)**

**Infinera (Coriant), ABB (Keymile):**

- Delivery and installation of SDH equipment for nationwide transport network
- Technical support for maintenance of SDH equipment
- Delivery and installation of PDH multiplexer equipment (ongoing project)
- Delivery, installation and implementation of DWDM equipment for nationwide transport networks

Figure 1 – <http://www.roamingnetworks.com/wp-content/uploads/2021/08/RN-INC-General-Presentation-v5.6-06082021.pdf>

**STRATEGIC PARTNERSHIPS**

Strategic decision of the company to extend its field of operations into the Enterprise Market resulted in creating strategic partnership with Coriant and Huawei.

In 2011, Roaming Networks signed Value Added Reseller agreement with Coriant (ex Nokia Siemens Networks-NSN) for an Enterprise Market.

In 2013, Roaming Networks signed Value Added Partner agreement with Huawei for an Enterprise Market.

Figure 2 – <http://www.roamingnetworks.com/wp-content/uploads/2021/08/RN-INC-General-Presentation-v5.6-06082021.pdf>

- <sup>1</sup> <https://srdjanoggo.rs/a-stolen-country-the-us-elections-and-what-comes-next/>
- <sup>2</sup> [https://www.roamingnetworks.com/?page\\_id=107&lang=en](https://www.roamingnetworks.com/?page_id=107&lang=en)
- <sup>3</sup> <https://www.cins.rs/en/company-belonging-to-nenad-kovac-thrown-out-of-business-in-denmark/>

## DOMINION VOTING SYSTEMS

Dominion Voting Systems Corporation is located at OSMANA DJIKICA 18, 11060, Beograd Serbia.<sup>4</sup> It is registered as a Computer Systems Design company.<sup>5</sup> One of the software engineers is **Ivan Yukovic**, designing Election Management Systems (EMS) used in U.S. elections. **Srđan Nogo**, a former Serbian Member of Parliament, identified connections between Serbian government, tech companies, George Soros, and the former VP Joe Biden.<sup>6</sup> He confirmed Dominion used the Serbian company as their software design team. As he began writing about the US election and his discoveries about where the Dominion software was actually designed and maintained, **Bojan Djordjevic**, listed as the legal representative of the Serbian company, began responding to him and trying to explain.<sup>7</sup>

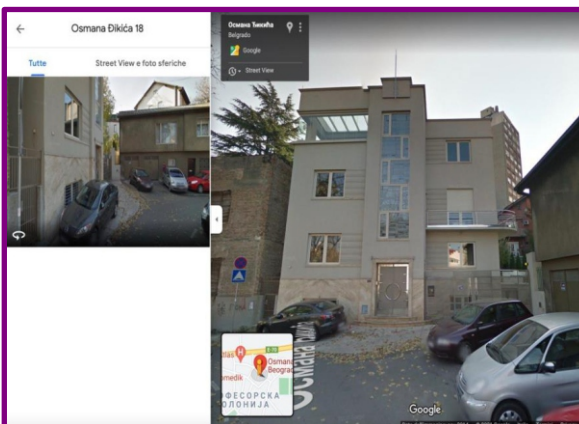


Figure 3 – <https://goo.gl/maps/AsPki-3Y5eaDwXHKUa>

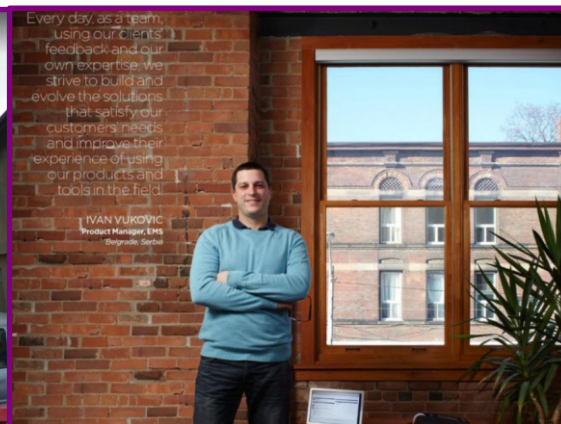


Figure 4 – formerly hosted on Dominion website prior to 2020 election

Source: Joe Oltman Presentation Cyber Symposium

<sup>4</sup> <https://www.dnb.com/business-directory/company-profiles/dominion-voting-systems-corporation-%28europa%29-oqranak-beograd-%28paullula%29.9a0c6dfa28b4af3111f4dce6ca6274e.html>

<sup>5</sup> *ibid*

<sup>6</sup> <https://srbin.info/svet/the-serbian-software-and-the-election-fraud-in-usa/>

<sup>7</sup> *ibid*

# HUAWEI, THE CHINESE TECH DRAGON

On May 16, 2019, the United States BIS added Huawei Technologies Co., Ltd. and many of its non-U.S. affiliates to the Entity List.

## 1) Why did BIS add Huawei to the Entity List?

BIS added Huawei Technologies Co., Ltd. (Huawei) and many of its non-U.S. affiliates to the Entity List effective May 16, 2019 on the basis of information that provided a reasonable basis to conclude that Huawei is engaged in activities that are contrary to U.S. national security or foreign policy interests and its non-U.S. affiliates pose a significant risk of involvement in activities contrary to the national security of the United States. This information included the activities alleged in the Department of Justice's public Superseding Indictment of Huawei, including alleged violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA by providing prohibited financial services to Iran, and obstruction of justice in connection with the investigation of those alleged violations of U.S. sanctions. Effective August 19, 2019, BIS added another 46 non-U.S. affiliates of Huawei to the Entity List because they also pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States.

Figure 5 – <https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file>

The addition of Huawei and its affiliates to the Entity List imposed a license requirement on the listed entities supplemental to those found elsewhere in the Export Administration Regulations (EAR).<sup>8</sup>

<sup>8</sup> <https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file>

## AMERICAN "VOTING" WITH CHINESE CHARACTERISTICS

Dominion Voting Systems uses Roaming Networks, the Serbian Huawei partner: *Implementation all flash Pure storage solution on primary Data Center.*<sup>9</sup> And Dominion hardware is Made In China. So how much Huawei related technology may be present in either the data center or the election equipment? And who does the testing of this Chinese sourced hardware?

### References

#### CT Infrastructure and Data Center

- Tehnomanija**
  - Data Center and computer network
- Republički fond PIO Srbije** (Network resource expansion)
  - Implementation of new network equipment
- Telekom Srbija**
  - TK Centar Belgrade, delivery of the equipment and installation of the low voltage supply system
- m.tel Banja Luka**
  - Primary Data Center, delivery and implementation of complete power supply system and system for distribution of electric power
- m.tel Podgorica**
  - Complete adaptation of Data Center Niksic
- Dominion Voting**
  - Implementation all flash Pure storage solution on primary Data Center

Figure 6 – [https://www.roamingnetworks.com/?page\\_id=107&lang=en](https://www.roamingnetworks.com/?page_id=107&lang=en)



Figure 7 – Sacramento California election warehouse

**Potential Involvement of China  
In Testing and Approving Use of Dominion Voting Machines**

**Shenzhen Zhongjian Nanfang Testing Co., Ltd., Tied to Xiamen Institute of Building Science, ("XMABR") a State-Owned Chinese Communist Party Functionary**

Smartmatic International Corporation ("SIC") used Chinese-based testing companies for its software components since 28 December 2015. These include Shenzhen Zhongjian Nanfang Testing Co., Ltd., as well as another company known as NTEK Testing Technology Co., Ltd., telephone number 86-0755-61156599. The tester was identified as Lu Brown ([lbrown@ntek.org.cn/](mailto:lbrown@ntek.org.cn/)).

A third company identified as Siemic, Headquartered in Silicon Valley, San Jose, California, with superior facilities in San Jose (CA), Milpitas (CA), Nanjing(China), Shenzhen (China) and branch offices in Beijing (China), Shanghai (China), Taipei (Taiwan), SIEMIC is truly one-stop shop for compliance testing (ISO 17025) and product certifications (ISO Guide 65) for worldwide market access. Its facilities in China are located at Suite 311, Building 1, Section 30, No.2 Kefa Road, Science and Technology Park, Nanshan District, Shenzhen, Guangdong 518057, CN, and 2-1 Longcang Dadao, Yuhua Economic Development Zone, Nanjing, Jiangsu 210019, CN.

SEIMIC did two of the inspections, 13 December 2016 and 28 December 2015.

<sup>9</sup> [https://www.roamingnetworks.com/?page\\_id=107&lang=en](https://www.roamingnetworks.com/?page_id=107&lang=en)

importkey.com		BILL OF LADING		BOL : OOLU2639303621	
SUPPLIER/SHIPPER		BUYER/CONSIGNEE			
SHINING FAIR ENTERPRISES CO LTD 9F NO 669 BANNAN ROAD ZHONGHE DI NEW TAIPEI TW		DOMINION VOTING SYSTEMS INC 2010 N REDDUB BLVD SUITE 110 MCKINNEY TX 75060 US			
ORIGIN	DESTINATION	PLACE OF RECEIPT			
57076 Yantai, China	2709 Long Beach, California	SHENZHEN			
NOTIFY PARTY NAME	BILL TYPE	House Bill	BOL		
	HOUSE BILL	CROISZDAL3526996	OOLU2639303621		
Actual Arrival Date	Vessel Name	Container Number	Estimate Arrival Date	Vessel Country Code	
2020-06-27	RIO GRANDE	OOCU7625182	2020-06-27	US	



## Deep Dive into Utah Voting Systems

What Americans witnessed during the 2020 November Elections brought election integrity and election security to the forefront of political issues. One of the main concerns was the voting systems themselves being a possible cause of election fraud. While the focus was on Dominion, all Voting System Manufacturers (VSM) use the same basic source code/software from license contracts and acquisitions. The following is just one example. In 2006 Representative Carolyn B Maloney submitted letter of concern regarding Smartmatic, a foreign-owned company that is today headquartered in London, UK<sup>1</sup>, acquired Sequoia from Diebold.<sup>2</sup> Later Smartmatic announced in November of 2007 the sale of Sequoia Voting Systems, Inc (Sequoia).<sup>3</sup> An April 2008 court case regarding Hart InterCivic acquiring Sequoia Voting Systems, Inc revealed a license agreement between Sequoia and Smartmatic who owns the patent to vote-counting software.<sup>2</sup> When Hart InterCivic failed to acquisition Sequoia, Dominion Voting Systems Inc (Dominion, Inc) acquired Sequoia in 2010. Prior to this in 2010, the Justice Department anti-trust suit against Election Systems & Software (ES&S) resulted in sale of Premier Election Solutions, Inc. (formerly Diebold) to Dominion.<sup>4</sup> Dominion also entered a license agreement for AutoMark voting terminals from Elections Systems and Software (ES&S).<sup>5</sup> So let's review. Diebold sold Sequoia to Smartmatic to become Smartmatic-Sequoia. Once it became public that Smartmatic was a foreign owned company, it moved Smartmatic-Sequoia to US investors becoming Smartmatic Voting Systems, Inc based in Florida. Smartmatic then tried to sell to Hart InterCivic, but this fell through due to the inability of Hart InterCivic to acquire the vote-counting software in full from Smartmatic. In 2010, Dominion acquired Sequoia Voting Systems, Inc. Another acquisition by Dominion in 2010 was the result of anti-trust suit that required ES&S to sell Premier Elections Solution, Inc (formerly Diebold). Do you see just how these companies and the software/source code intertwine?

You also must look at acquisitions of the source code and/or features. On November 1, 2004 a Wired report "E-Voting Tests Get Failing Grade" went through the history of I-Mark Systems which was created by Bob Urosevich.<sup>6</sup> Both Bob and Todd Urosevich are intertwined in the US elections systems companies.<sup>7</sup> I-Mark was purchased by Global Elections Systems in 1997 then Diebold in 2002.

---

<sup>1</sup> Smartmatic. (2021). *Smartmatic Our History*. <https://www.smartmatic.com/us/about/our-history/>

<sup>2</sup> Maloney, C. (2006). *Letter to Henry M Paulson, Jr, Secretary Department of Treasury*. [https://maloney.house.gov/sites/maloney.house.gov/files/documents/financial/acquisitions/20061006ElectionsCFIUS\\_paulson.pdf](https://maloney.house.gov/sites/maloney.house.gov/files/documents/financial/acquisitions/20061006ElectionsCFIUS_paulson.pdf)

<sup>3</sup> Maloney, C. (2007). *Smartmatic Announces Sale of Sequoia Voting Systems*. <https://maloney.house.gov/media-center/press-releases/smartmatic-announces-sale-sequoia-voting-systems>

<sup>4</sup> Justice News. (2010). *Justice Department Requires Key Divestiture in Election Systems & Software/Premier Election Solutions Merger*. <https://www.justice.gov/opa/pr/justice-department-requires-key-divestiture-election-systems-softwarepremier-election>

<sup>5</sup> Dominion Voting. (2010). *Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets from ES&S Press Release*. [https://www.bradsblog.com/Docs/DominionAcquiresPremierReleaseFinal4\\_051910.pdf](https://www.bradsblog.com/Docs/DominionAcquiresPremierReleaseFinal4_051910.pdf)

<sup>6</sup> <https://www.wired.com/2004/11/e-voting-tests-get-failing-grade/>

<sup>7</sup> [https://www.protectourvotes.com/wp-content/uploads/FINALDRAFTVotingMachineCompanyMegaThreadPart1.pdf?\\_\\_cf\\_chl\\_jschl\\_tk\\_\\_=pmd\\_8012b18ca3a0419e2d04ae9539ad6bc0bf94a44e-1626811200-0-gqNtZGzNAiKjcnBszQji](https://www.protectourvotes.com/wp-content/uploads/FINALDRAFTVotingMachineCompanyMegaThreadPart1.pdf?__cf_chl_jschl_tk__=pmd_8012b18ca3a0419e2d04ae9539ad6bc0bf94a44e-1626811200-0-gqNtZGzNAiKjcnBszQji)

A licensing issues was blamed for the issues in the 2010 Philippine elections.<sup>1</sup>

Smartmatic has had to admit system errors of its technology in the compact flash card (CFC) fiasco during the May 3, 2010 final testing and sealing (FTS) or a week before the May 2010 elections in the Philippines. It blamed Dominion's software for failing to correctly read and record the paper ballots.

The Venezuelan company accused Dominion of breaking the 2009 license agreement by failing to deliver "fully functional technology" for the 2010 Philippine elections, and failing to place in escrow the required source code, hardware design, and manufacturing data.

This is an explicit admission by Smartmatic of the "failure of its system to function fully, resulting in glaring errors, most of which were documented" by CenPEG and AES Watch in 2010, Dr. Pablo Manalastas, AES Watch co-convener and CenPEG Fellow for IT said.

"Does Dominion's failure automatically imply Smartmatic's failure to do the escrow required by the election law (RA 9369)?" Manalastas added. "Do these actions by Smartmatic constitute a criminal intent to cheat, a criminal intent to avoid its contractual obligations with Comelec and with the Filipino people?" he asked.

A congressional committee should probe why Smartmatic has been saying its system was 100 percent perfect contrary to the scientific studies of Filipino IT experts and scholars.

Through the suit we now know that the election technology used in the 2010 national elections was fraught with program errors and deficiencies – which CenPEG, along with the broad citizens election watchdog AES Watch have raised since 2009.

Another example of license issues can be found in the 14 Jan 2013 case Smartmatic International Corporation v. Dominion Voting Systems International Corporation.<sup>2</sup>

#### **B. Facts**

In October 2009, Dominion granted Smartmatic a worldwide (except for the United States and Canada) nonexclusive license to certain precinct count optical scan ("PCOS") voting systems that Dominion had developed (the "License Agreement" or the "Agreement"). The License Agreement granted Smartmatic rights to certain patents and patent applications that Dominion owned or controlled (the "Licensed Patent Rights") and to "all know-how, trade secrets, methodologies and other technical information owned or possessed by Dominion" (the "Licensed Technology").<sup>1</sup> The License Agreement contains a noncompetition provision. This provision limits Smartmatic's

---

<sup>1</sup> Clark Aff. Ex. A, PCOS Framework License Agreement ("License Agreement"), §§ 1.2 & 1.4. The full definition of Licensed Patent Rights, Licensed Products, and Licensed Technology is set forth *infra* Part II.B.4.a.

---

<sup>1</sup> <https://www.philstar.com/opinion/2012/11/10/864977/damning-evidence-against-smartmatic-pcos>

<sup>2</sup> <https://law.justia.com/cases/delaware/court-of-chancery/2013/ca-7844-vcp.html>

But these company acquisitions, common shareholders, and web of licensing agreements are not the only pattern found with US election systems. A great article from Harper's Magazine, "How to Rig an Election" lays out the connection between ES&S and Nebraska politics<sup>1</sup>. The same people move throughout the US voting system companies. Remember Smartmatic? Who was the voting system that Smartmatic replaced? Elections Systems & Software.<sup>2</sup> Nefarious. Maybe not, but it shows a pattern of conduct and the amount of influence the two Urosevich brothers have had, not just in US elections, but worldwide since the 1970's.

**The decision to replace the \$120 million system built by Omaha-based Election Systems & Software was made Feb. 16 under unusual circumstances. Two of the five National Electoral Council members sympathetic to the opposition complained that they had been largely shut out of the process.**

**"The selection process was secret and it didn't allow us to get any information about the bidders and their products," board member Sobelia Mejias said after the decision.**

**Other members knew about the government's investment, according to one member who asked not to be identified.**

**The new system is to be built by the Smartmatic Corp., which is incorporated in Florida, and programmed by Bizta, which also is registered in Florida and Venezuela.**

**Pro-Chavez government officials and company executives interviewed by The Herald say the Smartmatic-Bizta machines are among the most secure in the world, and that the government's investment in Bizta was unrelated to Bizta's bid for the voting machine contract.**

ES&S (Elections Systems & Software of Omaha, NE) are not just intertwined with software and acquisitions, but also by family. Two Brothers named Robert (Bob) and Todd Urosevich worked for Westinghouse Corporation in the voting machine division during the mid 1970's. The brothers founded Data Mark in 1979 with investments from by HF Ahmanson Co and Council for National Policy. In 1984 McCarthy & Company became majority shareholder and renamed to American Information Systems (AIS). In 1995, Bob Ursovech founded iMark. Global Election Systems, later Diebold/Premier, acquired iMark. In the same year, AIS acquired Election Systems & Software, a division of Business Records Corporation. AIS merged and became Election System & Software (ES&S) with Todd Urosevich as Director. At the same time Bob Urosevich was President of Diebold Elections Systems, Inc which was renamed to Premier Election Systems then purchased by ES&S who was required to divest, so Premier is sold to Dominion Voting Systems, Inc.<sup>3</sup> This further demonstrates how VSM are connected. Another interesting connection is that Bob Urosevich was on the Board of Directors of Scytl, an election reporting company.

Many think that election fraud issues with the voting systems was new to the 2020 elections. This is not the case. Year after year the same election fraud issues have been reported. In today's world of censorship researching errors

---

<sup>1</sup> <https://harpers.org/archive/2012/11/how-to-rig-an-election/5/>

<sup>2</sup> [https://www.bradblog.com/Docs/SequoiaSmartmaticLetter\\_Chicago\\_EdBurkeToLangdonNeal\\_011108.pdf](https://www.bradblog.com/Docs/SequoiaSmartmaticLetter_Chicago_EdBurkeToLangdonNeal_011108.pdf)

<sup>3</sup> <https://www.accesswire.com/471912/Voting-Technology-Companies-in-the-US--Their-Histories-and-Present-Contributions>

back to 2004 when across the nation states began using electronic voting systems. Excerpt from Phillip J Windley testimony to the Utah Voting Equipment Selection Committee on October 30, 2004<sup>1</sup>:

Some people believe that simply recording the vote on two different devices in the voting machine achieves the objective of creating an audit trail, but computer security experts know that this sort of plan is flawed. It's all too easy for the computer program, *regardless of how thoroughly it is tested*, to record the same mistake in two places. The only way to avoid this is to give the voter the control over a permanent copy, that can be deposited in a separate container for review if needed.

The State of Utah has approximately \$28 million to spend on developing or purchasing new voting systems. The State's Elections Office recently issued a request for proposals (RFP) for voting equipment. I along with over a dozen other local computer science professors and voting experts sent a formal response to the Elections Office citing over a dozen deficiencies. Among those deficiencies were two of special import:

- a.) The RFP does not require a voter verifiable paper ballot or any other kind of independent audit trail.
- b.) The RFP does not specify what security requirements the equipment will have to meet in sufficient detail or allow enough time to complete such a security evaluation of the proposed equipment.

I believe that the RFP process is well intentioned, but nevertheless seriously flawed. The correct way to conduct the RFP would be to have the security discussions up front and then to write an RFP that requires vendors to meet specific requirements. Because this wasn't done, the RFP process has inadvertently, I believe, hidden the equipment selection behind a wall of secrecy. Consequently, I and many others are concerned about the evaluation process, who will do the evaluation, and the believability of the results. Hiring friendly consultants to do the evaluation is not acceptable. The State should not be afraid to subject their choice to the most stringent evaluation process possible.

Below are two excerpts from an article on May 11, 2006 that explains security issues found in the electronic voting systems in Utah<sup>2</sup>.

Black Box Voting issued a [report](#) on the security of Diebold voting machines The investigation revealed security holes at the bootloader, OS, and application levels. The recommendations of the report were (quoting the report):

- Because there is no way of having chain of custody or audit trail for machines, the machines need to be reflashed with a known good version (assessing the risks potentially inherited). Ideally this should be done by the proper governmental authorities rather than being outsourced.
- After that, extensive chain of custody management has to be established to make sure that machines do not potentially get recontaminated. Less than five minutes is required for contamination.
- The bootloader needs to be re-engineered.
- The cases need to be properly and permanently sealed.

This study was done with information gathered when Emery Count (Utah) County Clerk Bruce Funk [allowed](#) security experts to examine his county's machines. Needless to say Diebold and Utah Elections officials weren't too happy he did this. His actions however, have resulted in the first real security data about these machines.

---

<sup>1</sup> [https://www.windley.com/docs/2004/voting equip\\_selection.pdf](https://www.windley.com/docs/2004/voting equip_selection.pdf)

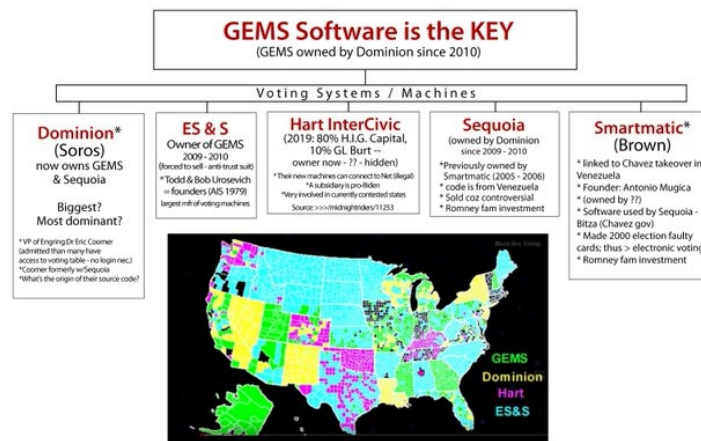
<sup>2</sup> <https://www.zdnet.com/article/voting-machine-security-flaws-uncovered/>

- First, these machines are new and the procedures that can catch problems are largely based on the old way of doing things. We just don't have much experience running elections with these kinds of machines. That will get better over time, but I'm always concerned about how election officials are countering the new threats.
- More importantly, in the past a single election worker had control over a relatively small portion of the overall election and getting control over large parts of the election required a larger conspiracy. Law enforcement loves large conspiracies because they always break down somewhere. By introducing computers, we've potentially increased the reach of a single person to a larger part of the election system.

Should we panic? No. But we ought not to dismiss this security concern out of hand either as Diebold seems to hope we will. More states should subject more voting machines to

independent tests by real computer security experts. If there's nothing to hide, then this should be a relatively painless thing to do. The fact that Diebold and other manufacturers are so unwilling to be forthcoming about the security of their machines leads me to wonder what they're worried about.

Other issues were found around the country. A 2004 Mother Jones article “Diebold’s Political Machine” exposes the connection between Diebold Election Systems of Ohio and Election System and Software of Nebraska<sup>1</sup>. March 20, 2008 Computerworld reported that clerks in New Jersey found issues with the vote count on Sequoia voting systems.<sup>2</sup>



Map Source: Fraction Magic - Detailed Vote Rigging Demonstration  
Beverly Harris - <https://www.youtube.com/watch?v=Fob-AggZn44> - Oct 31, 2016

\*Diebold/DES/Premier owned GEMS until 2009, when it was sold to ES&S, then to Dominion in 2010 (due to an anti-trust suit)  
\*\*Smartmatic is not on this map because it has had a non-compete clause with Dominion not to do business within the United States  
Source: <https://www.potteranderson.com/delawarecase-77.html>

#### FINDINGS SO FAR

Voting software & hardware is in the hands of a small gp of companies run by people who have worked together in the industry for years. All have been involved in voter fraud issues. Dominion seems to be the most dominant but all are highly influential & have strong ties to one another and to gov't structures at all levels plus top agencies (e.g., CISA & Homeland Security)

VERSION 4. 11-15-2020

<sup>1</sup> <https://www.motherjones.com/politics/2004/03/diebolds-political-machine/>

<sup>2</sup> <https://www.computerworld.com/article/2537855/after-threats--nj-clerks-call-for-e-voting-investigation.html>

A key issue with election integrity and our current voting systems is the Global Election Management System or GEMS.<sup>1</sup> Because of the intermingling of companies and licensing, GEMS source code can be found many US election systems. This 2016 video “Fractional Voting” by Bev Harris explains the GEMS issue that is key to fractional voting and vote rigging. <https://videopress.com/v/18LiSPWI>.

The following is how GEMS relates to Utah’s voting systems:

Salt Lake County uses Dominion Voting Systems GEMS v.1.21.6.0<sup>2</sup> the Global Election Management System (GEMS).

The information below is the safe diebold/ dominion version upgrades that we purchased in 2012 and installed in 2013. They only thing that we installed since then was a new certificate that allowed us to keep using the software/firmware.

**Information:**

**Touchscreen**

- Diebold AVTSX Build Number 4.7.10

**Ballot Scanner**

Photscribe PS900 v2.6.2

**Tabulation Software**

- Dominion Voting Systems GEMS v1.21.6.0
- Premier Election Systems PCS v2.2.5.0

**Electronic Poll Books Hardware**

- Apple iPad (6th Generation)

**Electronic Poll Books Software**

- KNOWiNK PollPad3 v2.5.0

Thank you,

Lannie



**Lannie K. Chapman**  
Chief Deputy Clerk  
Salt Lake County Clerk  
[LKChapman@slco.org](mailto:LKChapman@slco.org)  
385-468-7420



Diebold Elections Solutions Uses GEMS software.<sup>3</sup>

DESI Help Desk/ Server Configuration Support

DESI maintains a help desk in the McKinney, TX office which will be available to every support person and election official throughout the State Contract. The help desk will be an extension to the Project Management Office in Utah. The DESI help desk will configure and test the 29 GEMS servers for installation in the 29 Utah counties and in the Utah Lt. Governor’s office. The configurations will begin once the contract has been signed and the servers are ordered. The help desk staff has extensive knowledge and experience with server configurations and testing. They will perform the following:

- Installing all hardware to include digi board and sound card
- Install Windows Operating System 2000 Server Software
- Apply Updates
- Upload all 3<sup>rd</sup> party software
- Install GEMS software
- Configuration of Security and Communication Settings
- Apply testing to system to check for errors

<sup>1</sup> <https://pbs.twimg.com/media/EnSAJapWMAQtyce.jpg>

<sup>2</sup> Salt Lake County GRAMA email

<sup>3</sup> Found in 2005 Diebold Contract AR1910 found using Box Elder County filing cabinet to research Box Elder County's Resolutions, Ordinances & Contracts using key word “Diebold” and click on HAVA: <http://www.boxeldercounty.org/resolutions-ordinances-contracts.htm>

Diebold, Inc the parent company to Diebold Election Systems, Inc (DESI), renamed DESI to Premier Election Solutions, Inc after system malfunctions were widely reported during 2004 and 2008 elections. Election Systems & Software (ES&S) acquired Premier Election Solutions, Inc on September 2, 2009.<sup>1</sup>

Unfortunately this put ES&S over 70% of VSM market. DOJ filed an anti-trust suit against ES&S.<sup>2</sup> This resulted in Dominion Voting Systems, Inc, a subsidiary of Dominion, Inc a Canadian Company, acquiring Premier Election Solutions in 2010.

Dominion acquisition of Premier Election Solutions Assets included GEMS.<sup>3</sup>

**dominion** | VOTING<sup>®</sup>  
221 Hopkins Avenue  
Jamestown, New York 14701

May 19, 2010  
FOR IMMEDIATE RELEASE

For Information Contact:  
Dominion Voting Systems  
404-955-9799  
[media@dominionvoting.com](mailto:media@dominionvoting.com)

### **Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets From ES&S**

*Transaction Approved by the U. S. Department of Justice, Will Significantly Increase Competition in the United States Voting Systems Industry*

*Dominion's Engineering and Customer Service Expertise Will Support Premier's Voting Products Throughout the U.S.*

**JAMESTOWN, New York** .... Dominion Voting Systems, Inc. today announced that it has acquired from Premier Election Solutions, Inc. (Premier) a wholly owned subsidiary of Election Systems and Software (ES&S), the primary assets of Premier, including all intellectual property, software, firmware and hardware for Premier's current and legacy optical scan, central scan, and touch screen voting systems, and all versions of the GEMS election management system.

As part of the transaction, Dominion also acquired an irrevocable, perpetual license for the AutoMark voting terminals used by voters with disabilities, a similar license for the VoteRemote absentee vote-by-mail processing solution, and rights to spare parts, supplies and other resources necessary to support and service these installed systems. In addition, Dominion will acquire a percentage of existing Premier inventory.

---

<sup>1</sup> Kitten, T. (2009). *Diebold sells U.S. elections system business to ES&S, maintains ownership of elections business in Brazil*. ATM Marketplace. <https://www.atmmarketplace.com/news/diebold-sells-us-elections-systems-business-to-ess-maintains-ownership-of-elections-business-in-brazil/>

<sup>2</sup> Friedman, B. (2013). *Diebold Charged With Bribery, Falsifying Docs, "Worldwide Pattern of Criminal Conduct"*. Truthout. <https://truthout.org/articles/diebold-charged-with-bribery-falsifying-docs-worldwide-pattern-of-criminal-conduct/>

<sup>3</sup> Dominion Voting Systems, Inc. (2010). *Press Release: Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets from ES&S*. <https://web.archive.org/web/20100704220058/http://dominionvoting.com/images/pdfs/DominionAcquiresSequoiaFinal.pdf>

Salt Lake County used Dominion Voting Systems in 2020 elections. 2011 AR1910 RFP shows the company history of new contract to Dominion Voting Systems, Inc and GEMS Software License Agreement.<sup>1</sup> According to GRAMA, SLCO did not use the 2018 AR1910 RFP<sup>2</sup> to purchase upgrade Dominion Voting Equipment prior to 2020 election.

## STATE OF UTAH CONTRACT ASSIGNMENT

### STATE CONTRACT # AR1910

1. PARTIES TO THE ASSIGNMENT:

ASSIGNOR (old contractor): Premier Election Solutions  
 ASSIGNEE (new contractor): Dominion Voting Systems, Inc.  
 NEW VENDOR NUMBER:  
 (Assigned by the State of Utah)

**Assignee please complete company information form:**

Dominion Voting Systems, Inc.			27-0565149	
Company Name			Federal Tax ID #	
1201 18 <sup>th</sup> Street, Suite 210		Denver	CO	80202
Ordering Address		City	State	Zip Code
Dept. 1241, PO Box 1070		Charlotte	NC	28201-1070
Remittance Address (if different from ordering address)		City	State	Zip Code
<input checked="" type="checkbox"/> Corporation	<input type="checkbox"/> Partnership	<input type="checkbox"/> Proprietorship	<input type="checkbox"/> Government	Tuyet Ha
Company Type			Company Contact Person	
(866) 654-8683		(303) 291-3909		
Telephone Number		Fax Number		
www.dominionvoting.com		ar-dvsi@dominionvoting.com		
Internet Home Page		Email Address		

2. CONTRACT SERVICES ASSIGNED TO ASSIGNEE (Brief Description):

This is the contract assignment of the State of Utah and Premier Election Solutions, Inc. contract entered into on August 11, 2005 and amended on February 17, 2010. The Statewide Contract is Contract Number AR1910. As part of the assignment, Dominion agreed to provide a software license for the continued use of the system at discounted rates.

3. ASSIGNEE agrees to perform all of ASSIGNOR'S contract responsibilities, and to abide by all contract provisions specified in this contract. ASSIGNOR will have no further responsibilities to perform under this contract and will make no claim for benefits arising from this contract after the effective date of this assignment.

EFFECTIVE DATE: 05/10/2011.

<sup>1</sup> 2011 RFP AR1910 from Salt Lake County GRAMA

<sup>2</sup> 2018 RFP can be found using Utah Purchasing Division Approved Vendor Search



## A G R E E M E N T

**1. Incorporation of Recitals.** The above recitals are true and correct and incorporated herein by this reference as if fully set forth.

**2. Amendment Language.** The terms of this Amendment shall modify and supersede any and all inconsistent terms of the Agreement. Except as specifically set forth in this Amendment, all remaining applicable terms and conditions of the Agreement shall remain in full force and effect.

**3. GEMS Software License.** Exhibit B to the First Amendment to Contract and Exhibit B of Attachment C to the Original Contract are hereby amended by reducing the Annual Software License and Maintenance Fee for the GEMS software from \$193,500.00 to \$93,500.00. The GEMS Software License Fee for 2011 shall be pro-rated based upon the Effective Date of this Amendment.

**4. Notices.** Section 10 of the First Amendment to Contract and Section 14.6 of Attachment C to the Original Contract are hereby amended by deleting the Notice to DESI provision and replacing it with the following:

“If to Dominion:

Dominion Voting Systems, Inc.  
1201 18<sup>th</sup> St. Suite 210  
Denver, CO 80202  
Attn: Office of General Counsel”

Amendment to Assignment Agreement  
Dominion Voting Systems Inc. & State of Utah

Page 1 of 2  
05.11.2011

2017 ES&S RFP page 98-99 states currently “counties upload their data from a central location using GEMS to send data to the State”. VISTA integrates with GEMS data. GEMS software “has developed an upload feature to take the GEMS data and process it into VISTA.” Salt Lake County kept the “current” system noted in RFP, therefore it assumes the same process was used in 2020 elections. <sup>1</sup>

Q: How many counties use modems for the transmission of election night results from the polling location to the EMS? Which counties use modems?

Question added by: Dora Chan 5/24/2017 8:24 AM

A: No counties use modems. Nothing comes from a polling location. All counties upload their data from a central location using GEMS to send the data to the State.

Answered by: Windy Aphayrath 5/25/2017 2:01 PM

A: Currently the State uses GEMS software and has developed an upload feature to take the GEMS data and process it into VISTA. In Group 3.3 the State seeks to understand the proposed system's capabilities regarding importing and exporting data. The State expects to work with the chosen Offeror to adapt existing systems, but seeks to understand the mechanism Offerors use to export/import data. Offerors should provide details on the structure of the proposed system, how ballot information is generated, mechanisms for importing and exporting data, customization options, and the ease to which the system can be adapted.

Answered by: Windy Aphayrath 5/25/2017 1:56 PM

---

<sup>1</sup> ES&S RFP. (2017) From State Elections office GRAMA

Dominion Assure 1.3 EAC Modification Test Plan states it GEMS AV-OSX was updated<sup>1</sup>



### **1.8.1 GEMS**

GEMS was updated to account for the following:

- The Cards Cast report was updated to resolve an issue where the total number of registered voters was not accurately reported for split precincts.
- An occasional poster sharing violation was leaving the application in a state that did not accurately reflect the status of the memory card information being uploaded. The system accumulates the data in a two step process where the data is uploaded from the memory card and then posted to the database. If the upload was successful then the green arrow was displayed, even if the posting failed.
- An installation program was updated with a new splash screen and agreements page to reflect Dominion Voting Systems instead of Premier Election Solutions.
- A runtime error is addressed by a documentation update implemented to prevent the runtime error from occurring. The error was caused by permissions for a folder not having inheritable right propagated to its sub-folders.

### **1.8.2 AV-OSX**

AV-OSX was updated to account for the following:

- The Protective System Counter (PSC), which counts the total number of ballots ever cast on the machine, as opposed to the ballots cast for a specific election, was archiving the PSC only during graceful shutdowns. A hardware reset was reverting the PSC to its previously saved count without the current count being archived.
- Date presented on results tape can be incorrect, as it was using the system date (UTC) instead of the local date

---

<sup>1</sup> SLI Global Solutions. (2012) Dominion Assure 1.3 EAC Modification Certification Test Plan. [www.eac.gov](http://www.eac.gov)

Even with the updates, Texas Secretary of State tested and rejected certification of Dominion Voting System Assure 1.3. One issue was the GEMS security and tallying of votes.<sup>1</sup> Read more in Voting System Examination Dominion Voting Systems Assure 1.3.<sup>2</sup>

5. **Access to the Operating System.** Texas rules require that there be no access to the operating system (in this case Windows) during tabulation. Although GEMS enforces this, it is implemented using features of Microsoft Windows, and can be turned off by anyone with Windows administrative rights, provided GEMS has not been started. (Once GEMS has been started, it is no longer possible to defeat this.)

According to Dominion they have taken these actions to address the problem: (a) shipping systems that are properly configured, (b) publishing procedures for properly configuring Windows, and (c) restricting Windows administrative rights.

This is not sufficient in my opinion.

Item (a), above, is not that helpful, because not every customer purchases the hardware from Dominion.

Item (b) is not practical, because the required steps fill a nine-page, single-spaced document entitled "Protecting Windows 2003 Server for Texas's (sic) GEMS server," which present quite a challenge to typical jurisdictions. The steps are not simple ones. For example, on page 2 in the section labeled "Explorer," the second step is "Allow Running Only Certain Applications." The allowed applications are not specified, and no further details are given. I am a longtime Windows user who holds a Ph.D. in computer science, and I would need reference materials or other help to figure out how to do that.

On the other hand, the instructions on pages 5 - 7 can be accomplished relatively quickly by following the six detailed steps on page 5.

Item (c) does help somewhat by restricting the people who can tamper with the system to those who have administrative rights, but it still does not meet the requirement.

Restricting operating-system access is not a critical security feature, but it is required in Texas, and the procedure is so onerous that I doubt it is often carried out. GEMS should ensure compliance by refusing to tally real votes unless operating system access is actually disabled. (For example, when GEMS starts, it could check that the proper Windows settings are actually in force, so that OS access is known to be actually disabled. If they are not in force, GEMS could refuse to run.)

6. **Real-time Paper Audit Log.** Texas has a requirement for a real-time audit log on a continuous-feed printer. GEMS has a paper audit log, but it does not meet the Texas requirements. Texas requires that the tabulation system stop working whenever any log entry cannot be printed as soon as the event occurs. (This is the meaning of *real time*.) Also, any interruption in the real-time logging must itself be logged.

Here are the technical details: During the exam, we took the printer offline and demonstrated that GEMS continued to function. Only when we put the printer back online, did it print the log entries. The taking of the printer offline was not logged. In another test, we took the printer offline while a number of events occurred. Then we switched the power to the printer off and then back on. While the printer was powered off, GEMS refused to process anything and a prominent message was displayed explaining the problem. However, GEMS permanently lost the log entries for all the events that occurred while the printer was offline, and the fact that the printer was offline and then powered off was itself not logged.

This is not a critical security feature, in my opinion, but it is explicitly required in Texas, and the Dominion GEMS system does not comply.

---

<sup>1</sup> Texas Secretary of State. (2012). *Voting System Certification Evaluation Report: Dominion Voting Systems ASSURE 1.3*. [https://www.sos.texas.gov/elections/forms/sysexam/2012aug\\_berger.pdf](https://www.sos.texas.gov/elections/forms/sysexam/2012aug_berger.pdf)

<sup>2</sup> Sneeringer, J. (2012). *Voting System Examination Dominion Voting Systems ASSURE 1.3*. [https://www.sos.texas.gov/elections/forms/sysexam/2012aug\\_sneeringer.pdf](https://www.sos.texas.gov/elections/forms/sysexam/2012aug_sneeringer.pdf)

In 2007, Diebold election management system GEMS was evaluated. It found GEMS “susceptible to common errors and anomalies”, “lacks constraints that ensure election integrity”, GEMS allowed negative numbers where only positive numbers should be, Microsoft JET/Microsoft Access is too basic and “can be used by custom programs to access the data through the Microsoft Data Access Components Applications Programming Interface (MDAC API)”.<sup>1</sup>

## 2. Second Normal Form (2NF)

The overarching purpose of the Second Normal Form (2NF) is to reduce the amount of redundant and duplicate entries within a DB. A DB table satisfies 2NF if (a) it conforms to 1NF and (b) each non-primary key element is dependent upon the primary key.<sup>19</sup> DB satisfaction of 2NF means tables with repeating information separate the repeating data and reference those records through the use of “integrity constraints.” Integrity constraints provide a method to ensure data entry changes or updates do not result in a loss of data consistency.<sup>20</sup> The most common tool deployed is known as a foreign key

The first and second Normal Forms contain the most fundamental design principles for efficient and accurate DBs. Any DB that fails to satisfy the first two Normal Forms will suffer various failures upon deployment.

## B. System Technology Flaws: Use of JET

Microsoft’s Joint Engine Technology (JET) is a basic DB engine<sup>32</sup> technology that is appropriate for personal computing and very small scale applications requiring DB technology. Commercially known as Microsoft Access®, JET is a file-sharing DB that can support DBs with sizes up to 2 gigabytes.<sup>33</sup> JET is often considered ideal for small DB deployments with very few concurrent user/processes,<sup>34</sup> and can also be used by custom programs to access the data through the Microsoft Data Access Components Application Programming Interface (MDAC API).

But JET’s limitations have led Microsoft (MS) to state that JET is inappropriate for systems that require data integrity, security, and transaction logs and rollbacks.<sup>35</sup>

Microsoft JET ... was not intended (or architected) for the high-stress performance required by 24x7 scenarios, ACID transactions, or unlimited users, that is, scenarios where there has to be absolute data integrity or very high concurrency.<sup>36</sup>

An election management system obviously requires both “absolute data integrity” and in many urban jurisdictions if not all, a “very high concurrency” of users. Thus, the GEMS’ architects’ choice of inexpensive JET as the DB engine places the entire election tabulation process at very high risk.

---

<sup>1</sup> Ryan, T and Hoke, C. (2007). GEMS. [https://www.usenix.org/legacy/events/evt07/tech/full\\_papers/ryan/ryan.pdf](https://www.usenix.org/legacy/events/evt07/tech/full_papers/ryan/ryan.pdf)

In 2016, Bev Harris, author of *Black Box Voting* exposed GEMS<sup>1</sup> and Fractional Voting. In YouTube video *Fraction Magic—Detailed Vote Rigging Demonstration*, Harris exposes GEMS fractional counting in America. Harris said: “Imagine if the default setting is to hide the decimals. Right now, the GEMS is installed in counting votes in 25 states and 616 jurisdictions. Fractional counting began to migrate from GEMS into all other vendors. Voting systems, which count votes as fractions, may count as many as 99% of all American votes in 2016.”<sup>2</sup>

GEMS turned out to be a vote rigger’s dream. According to Harris’s analysis, it could be hacked, remotely or on-site, using any off-the-shelf version of Microsoft Access, and password protection was missing for supervisor functions. Not only could multiple users gain access to the system after only one had logged in, but unencrypted audit logs allowed any trace of vote rigging to be wiped from the record.

Other GEMS vendors include ES&S who acquired and owned GEMS from 2009-2010. ES&S Election Management Software (EMS) is ElectionWare.<sup>3</sup> All software components in EMS were listed in RFP.

- 3.1.5** Describe the proposed database system, including version identification. Identify all software components utilized by the EMS system, including customized vendor software, as well as others (e.g., Adobe) included and utilized by the EMS. ★

Text (Multi-Line)

- ElectionWare Election Management Software – v. 4.7.1.1 - Election Reporting Manager (ERM) – rev. 8.12.1.1 - RM/Cobol Runtime – v12.06 - Event Log Service (ELS) – v1.5.5.0 - Removable Media Service (RMS) – v1.4.5.0 - ExpressVote Previewer – v1.4.1.2 - VAT Previewer – v1.8.6.1 - Symantec Endpoint Protection – v12.1.6 - Cerberus FTP Server – v8.0.6 - Adobe Acrobat Standard – XI

---

<sup>1</sup> Collier, V. *How to Rig An Election*. <https://harpers.org/archive/2012/11/how-to-rig-an-election/5/>

<sup>2</sup> Harris, B. (2016) *Fraction Magic*. <https://youtu.be/Fob-AGgZn44>

<sup>3</sup> <https://www.essvote.com/products/electionware/>



# Dominion's Own FROG Destroys Their Claim

by [Tore Says](#) February 11, 2021

Dominion has been crying on television peddling the overused heart felt story about how the company started in a basement by Greek-Canadian Poulos. Same tiny violin. FROGS are potentially the downfall of ANY tech company's security not just Dominion.

Dominion's attorneys sent "intimidating" letters to various persons who filed affidavits exposing the company's deficiencies and warranted claims of malicious and intentional interference with the 2020 US elections. Sounds like witness intimidation or at the very least tampering with witnesses and evidence.

*Here's the truth. Dominion was created in John Poulos's basement in Toronto to help blind people vote on paper ballots. Its systems are certified under standards promulgated by the U.S. Election Assistance Commission ("EAC"). This involves a rigorous review and testing process conducted by independent laboratories accredited by the EAC, and Dominion designed the voting systems to be auditable and include a paper ballot backup to verify results. Because of these safeguards, there is overwhelming direct evidence that conclusively disproves claims about Dominion manipulating vote counts—namely, the millions of paper ballots that were audited and recounted by bipartisan election officials, confirming that Dominion accurately counted votes on paper ballots.*

*Part of intimidation letter*

Factually, HAVA ACT 2002 has been violated because the EAC has NOT certified them because the VSTLs were not certified. That's a topic for another matter.

This is where the technical terms come in and surely most post 2000 coders don't realize that "old ciphertexts" are the foundations of new ones and they were created with safe guards. In the case of Dominion which poetically means the power or right of governing is being owned by a real life and AI interpreter. In Sidney Powell's case an affidavit reveals that Dominion systems have a "cipher trapdoor". It's where code exists to translate plain text (info that you are transmitting to a receiver – like ballot votes to receiver for tally) into encrypted code and then encrypted code back into plain text. It's a FROG ciphertext. Ciphertext is basically encryption of plaintext (just naked data).

Block ciphers use logical operators or "eXclusive OR" (XOR) logic operators that are fixed sequences applied to plaintext and a secret key to yield ciphertext. FROG block ciphers are stealthy. They actually HIDE the actual fixed sequences or primitive operations even when the cipher is known. Normally the key is used as data but a FROG uses the secret key as data and also as a set of guidelines and instruction to create, combine or ALTER the data. That means the

Retrieved March 12<sup>th</sup>, 2021 from:  
<https://toresays.com/2021/02/11/dominions-own-frog-destroys-their-claim/>

secret key (decipher key) is used as a program – therefore FROG INTERPRETS the data as the KEY INSTRUCTS.

For example. Your ballot goes into the machine. The trapdoor “shuffles and cleanses” according to Dominion to anonymize your votes and spits them out on the other side “anonymized” to supposedly match your original data but without looking like the original data so you awarded privacy. You just have to trust them since you aren’t allowed to know their secret key. Is this why the EAC appointed companies and states aren’t allowed to examine the “proprietary code”?

They claim their software is proprietary because it’s about encryption – when in fact there is a FROG baked into it. Your ballot goes in as plaintext, a secret key encrypts it and then the same key decrypts it and then it comes out as plaintext again, so they say. FROG Ciphers use SECRET KEYS that are programs allowing to implement scripts and algorithms. Hence the percentage of votes and the change in tallies.

Incredibly, the creator of this block cipher attracted the Central Intelligence Agency back in 1998 because it was created to be able to DEFEND “itself” from unknown and unpredictable cyberattacks but also was a fail safe in case AI was ever to get out of hand. In essence, it’s the key to Quantum computing. The block cipher has come a long way from the original pitch below. How do I know? I was there in 1999 when the creators pitched it to former top brass namely, John Brennan, James Clapper, General Hayden, General Jones, John McCain and up and coming tech giants who use FROGS but unknowingly have the original FROG machine instructions baked into them.

*“FROG is very easy to implement (the reference C version has only about 150 lines of code). Much of the code needed to implement FROG is used to generate the secret internal key; the internal cipher itself is a very short piece of code. It is possible to write an assembly routine of just 22 machine instructions that does full FROG encryptions and decryption. The implementation will run well on 8 bit processors because it uses only byte-level instructions. No bit-specific operations are used. Once the internal key has been computed, the algorithm is fairly fast: a version implemented using 8086 assembler achieves processing speeds of over 2.2 megabytes per second when run on a 200 MHz Pentium PC.”*

Back then it was an algorithm with 8 cycles and a complicated for that time key schedule. Many worked hard as others have to amplify it and most AES block ciphers draw on the FALSE portrayal of what FROG was.

Building out a code is almost like a house that you build out, only ciphers are built out with subkeys upon subkeys but nevertheless the foundation remains the same. A FROG is simply a bidirectional interpreter. There is no master secret key UNLESS you know the ORIGINAL FROG block cipher key. That means EVERY FROG block cipher used is compromised because the master key is baked into it’s structure which was one of the unspoken and undetectable design flaws.



Retrieved March 12<sup>th</sup>, 2021 from:  
<https://toresays.com/2021/02/11/dominions-own-frog-destroys-their-claim/>

The text and original architecture has seemed to have vanished from books, papers and databases but a handful of people knew the actual core cipher. Incredibly, FROG was depicted as a weak key class when it wasn't. It's original architecture was not being discussed it was MISREPRESENTED and another faux version of it was "destroyed" so no one would look since the Agency took interest. They wanted to original architecture buried.

As far as Dominion lawsuits for defamation...*It seems that the FROGS will destroy them all.*

Dominion sent me a letter asking me to retract my article from 2019. Why? How does that article apply to them? They want me retract the math I did- and never mentioned their company. WHY? I am a FACT witness.

RECOVERED ARTICLE [HERE](#)

It is because they realized that I EXPOSED the actual inner workings. It exploits their "proprietary" information. Why would I retract the only evidence showing that their "proprietary" software isn't really proprietary if the master key exists?

Page 3 of 5

Retrieved March 12<sup>th</sup>, 2021 from:  
<https://toresays.com/2021/02/11/dominions-own-frog-destroys-their-claim/>

The master key is an algorithm that the Central Intelligence Agency purchased back in 1999 and I had the pleasure of learning it when it was running on 8 bit processors. I don't need a book or paper to remember the most incredible assembly routine that uses only 17 machine instructions that can complete FULL FROG encryptions and decryptions that are BAKED into all AES Encryption used across the world wide web. #OccamsRazor

The most incredible part of FROG is that you can't detect it because it is baked into every encryption algorithm because it's both a **key and program**. Almost like genetic crosstalk – it's quite genius. You don't have to use the Master FROG as a block cipher to exist. It's components are "spread across" ALL encryption algorithms today as they are basic machine instructions. Like the terminator, these components come together to form a FROG and run any script, manipulate and redirect data – undetectably when two or more components are accessed to trigger the cascade.

The FROG block cipher Dominion uses in their trapdoor was implemented by those that know how the master key works. Dominion may not even be aware that their secret key or their FROG isn't so secret as a way of creating non-attribution for those who do. Dominion being unaware is part of the non-attribution.

In the past decade China and Russia have been trying to determine the ultimate master key to all encryption. Considering that John Brennan, General Hayden and others know about it I wouldn't be surprised if they sold or lent a bootleg version of it simply to garner access undetectably into such systems. This was something that was tested in Ukraine that caused the voting systems to stall and hang – therefore they stopped counting. You can't run a master key program with too many or too little machine instructions because then the access will be terminated and severely flawed.

Make no mistake – this “proprietary” software has been used in all US and Global elections since 2000 with the “flavor of the month” Election Machine company.

Dominion is hiding behind “proprietary” information when in essence I exposed the existence of voting machine encryption being a **key and program** with my 2019 article they demanded I retract which didn't even mention them. Why? That is because their “proprietary” encryption isn't proprietary and the fact that you can't have ABSOLUTE proof that their KEY is only a KEY is evidence that it is a program and my math proves that without identifying the original FROG that can cause detrimental cyberspace chaos rendering AES and other encryption keys useless.

Regardless, Dominion's downfall will come from the CONGRESSIONALLY PASSED HAVA ACT 2002 that doesn't have Intellectual Property and “proprietary” argument loop holes to jump through. The EAC never certified them because those that certified them were NOT certified. The companies that “certified” Dominion are two – SLI GAMING and Pro V & V that lacked EAC certification. One has offices in CHINA and the other one is Jack Cobb who is WELL AWARE of the FROG component from his Defense contracting days. In other words, it seems that Dominion is guilty of intentionally breaching our national security by partaking in

*Page 4 of 5*

*Retrieved March 12<sup>th</sup>, 2021 from:  
<https://toresays.com/2021/02/11/dominions-own-frog-destroys-their-claim/>*

fraudulent elections since they KNEW they were not really CERTIFIED as HAVA ACT 2002 mandates.

*Page 5 of 5*

Voting Systems have many different aspects, one is Commercial Off The Shelf (COTS) components. COTS may make the VSM vulnerable. The following is an example of COTS in the EMS.<sup>1</sup>

★ Vendor Response Is Required

- Electionware Election Management Software – v. 4.7.1.1 - Paper Ballot – v. 4.6.1.0 - Event Log Service (ELS) – v1.5.5.0 - Election Reporting Manager (ERM) – rev. 8.12.1.1 - Removable Media Service (RMS) – v1.4.5.0 - ExpressVote Previewer – v1.4.1.2 - DS450 Central Scanner – v. 3.0.0.0, rev. 1.0 - DS850 Central Scanner – v. 2.10.2.0, rev. 1.0 - DS200 Central Scanner – v. 2.12.2.0, rev. 1.2, 1.2.3.0, 1.3 - ExpressVote Universal Voting System – v. 1.4.1.2, rev. 1 - DS200 Plastic Ballot Box - Balotar Ballot-on-Demand – v. Okidata C711 - COTS Adobe Acrobat Standard v. XI - COTS RMCOBOL v. 12.06 - COTS Symantec Endpoint Protection v12.1.6 - COTS Windows 7 SP1 - COTS Windows Server 2008 R2 SP1 - Cerberus FTP Server – v8.0.6 - Election Management System Hardware – \*System can vary based on solution architected. Standalone and Local Area Network (LAN) solutions are available. Minimum hardware requirements listed in section 3.1.20.

---

<sup>1</sup> 2018 WA17018 RFP Summary, Utah Elections Office GRAMA, p 53

# Do ES&S Have Modems?

Subject = Modem transmission

Public Thread

Q: How many counties use modems for the transmission of election night results from the polling location to the EMS? Which counties use modems?

Question added by: Dora Chan

5/24/2017 8:24 AM

A: No counties use modems. Nothing comes from a polling location. All counties upload their data from a central location using GEMS to send the data to the State.

Answered by: Windy Aphayrath

5/25/2017 2:01 PM

## Group 3.7: Security

### 3.7.1 Describe security measures/procedures for securely uploading vote count results to the EMS. ★

Text (Multi-Line)

• Both the Electionware election management system (EMS) and Election Reporting Manager (ERM) are installed on hardened systems and separated from both public internet and network access (unless otherwise stipulated). • Because these systems are password-protected via Microsoft Windows, as well as the Electionware and ERM programs, if security protocols are adhered to, the systems are protected from unauthorized access or manipulation. • Results are saved to USB flash drives and these flash drives are inserted into the PC housing Election Reporting Manager (ERM) to upload them into the software. • Files on the USB removable memory devices are digitally signed and encrypted with military-strength encryption: FIPS-compliant Advanced Encryption Standard (AES) encryption using a certified library from RSA. ES&S employs strong AES-128 and AES-256 encryption to FIPS 140-2 standards using the RSA BSAFE Library with ECDSA (Certificate 1058).

### 3.7.2 Describe security in place to protect for the audit logs. ★

Text (Multi-Line)

The Electionware Election Management System (EMS) audit log is stored in the password-protected database on a closed, hardened network. Only the election administrator may access the log via role-based access privileges. Equipment logs are digitally signed and brought into the EMS where they become part of the overall system log.

Subject = VISTA compatibility

Public Thread

Q: 3) In order to properly answer RFP question regarding interaction with VISTA in sections (3.3.1-3.3.3) offerors must better understand how VISTA is coded, works, and imports/exports information. The following is requested from the state: a. Flow charts of data flow in/out of VISTA b. Sample exports of ballot information c. Existing import formats currently accepted d. The ease with which UT IT Services can map new import formats e. Existing results file definitions/map f. Description of how VISTA stores/recalls/organizes ballot information that would be included in any import/export functions

Question added by: Daniel Chalupsky

5/24/2017 1:51 PM

A: Currently the State uses GEMS software and has developed an upload feature to take the GEMS data and process it into VISTA. In Group 3.3 the State seeks to understand the proposed system's capabilities regarding importing and exporting data. The State expects to work with the chosen Offeror to adapt existing systems, but seeks to understand the mechanism Offerors use to export/import data. Offerors should provide details on the structure of the proposed system, how ballot information is generated, mechanisms for importing and exporting data, customization options, and the ease to which the system can be adapted.

Answered by: Windy Aphayrath

5/25/2017 1:56 PM

**What the dispute is about:** The issue involves ES&S' DS200 precinct-based optical-scan machines, which come in two versions — one of which has an optional modem for transmitting results after an election.

**CYBERSECURITY**

## Election commission orders top voting machine vendor to correct misleading claims

This isn't the first time Election Systems & Software has faced accusations of making fabricated or misleading assertions about its voting machines.



A voter in a voting booth. | Steve Helber/AP Photo

By KIM ZETTER  
08/13/2020 05:00 PM EDT



The EAC certified the DS200 version without modem capability in 2009, but it has never certified the modem capability that comes with the second version, although the remaining components in that system are certified. In 2011, ES&S submitted a DS200 system with modem and network capability to the EAC for testing and certification, but after the testing lab created a protocol for evaluating this capability, ES&S withdrew those parts of the system from the testing plan; the remainder of the system was tested and certified without them in 2013.

ES&S markets the DS200 as an EAC-certified system, and in literature for the system it offers the modem capability as an optional feature — without indicating that the EAC has not certified this feature. Any component that is not EAC-certified and is added to an EAC-certified system effectively voids the certification of that system.

Under the EAC's testing and certification rules, manufacturers can label a system EAC-certified only if the whole system is certified. "The certification of individual components or modifications shall not be independently represented by a Mark of Certification," the EAC's certification manual says. The rules also require that a company's user manuals "warn purchasers that any changes or modifications to the system not tested and certified by the EAC will void the EAC certification of the voting system."



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

March 20, 2020

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

**Re: DS200 Misrepresentation**

Dear Mr. Pearson,

On January 7, 2020, the U.S. Election Assistance Commission (EAC) received a complaint from two organizations, Free Speech for People and National Election Defense Coalition, stating that:

1. ES&S may have violated Sections 5.14 and 5.15.1 of the EAC Testing and Certification Program Manual Version 2.0 by representing or implying that the DS200 with modem configuration is EAC certified when in fact only the DS200 without modem is EAC certified.
2. ES&S also may have violated Section 5.16 by failing to warn purchasers that adding a modem to the DS200 will void the EAC certification of the voting system in its entirety.

Sent via e-mail



April 3, 2020

**VIA EMAIL AND OVERNIGHT DELIVERY**

Jerome Lovato  
Director, Voting System Testing and Certification  
U.S. Election Assistance Commission  
1335 East West Highway, Suite 4300  
Silver Spring, Maryland 20910

**RE: Election Systems & Software, LLC ("ES&S") DS200® Modem Marketing Material Complaint**

Dear Mr. Lovato:

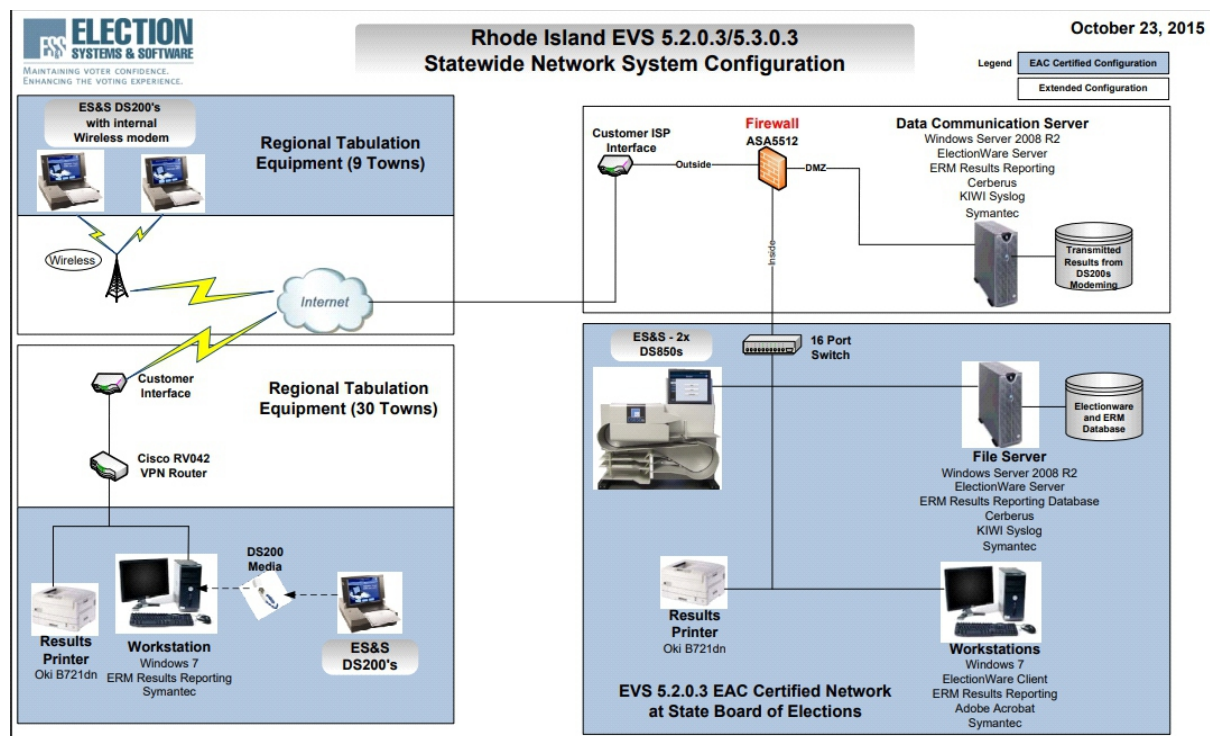
I am in receipt of your letter dated March 20, 2020, which sets forth certain findings by the Election Assistance Commission ("EAC") regarding ES&S' marketing materials for its

- ES&S has revised all of its DS200 marketing materials included on its website, as well as revised all print marketing materials for its DS200, to make it clear that the EAC has not certified the DS200 with the use of modeming;
- ES&S will send the enclosed letter to all of its DS200 customers who use the DS200 with modem, informing them that the DS200 with modem has not been certified by the EAC; and
- ES&S will post a notice to its customer portal advising all ES&S' customers that the DS200 with modem has not been certified by the EAC.

Internet Access also makes elections vulnerable. In September of 2020, ES&S had to correct misleading statements on the brochures that stated the DS200 were EAC certified and listed optional wireless modem results transfer with encryption.<sup>1</sup> To remedy, ES&S had to correct the brochure to reflect that adding a modem voids the EAC certification.<sup>2</sup>

We write to you to request that the Election Assistance Commission (EAC) initiate an inquiry and investigation into Elections Systems & Software (ES&S). ES&S may have violated, and likely continues to violate, Sections 5.14 and 5.15.1 of the EAC Testing and Certification Program Manual Version 2.0 (May 31, 2015) (TCPM)<sup>1</sup> by representing or implying that the DS200 with modem configuration is EAC certified when in fact only the DS200 *without* modem is EAC certified.<sup>2</sup> ES&S also may have violated Section 5.16 by failing to warn purchasers that adding an uncertified modem to the DS200 will void the EAC certification of the voting system in its entirety. The EAC should investigate this misconduct, require corrective action, and determine whether to suspend ES&S's manufacturer registration.

Examples of ES&S system for remote reporting capabilities for Rhode Island. Note that the election machine, DS200 is not connected to the internet, yet internet and remote reporting is utilized.



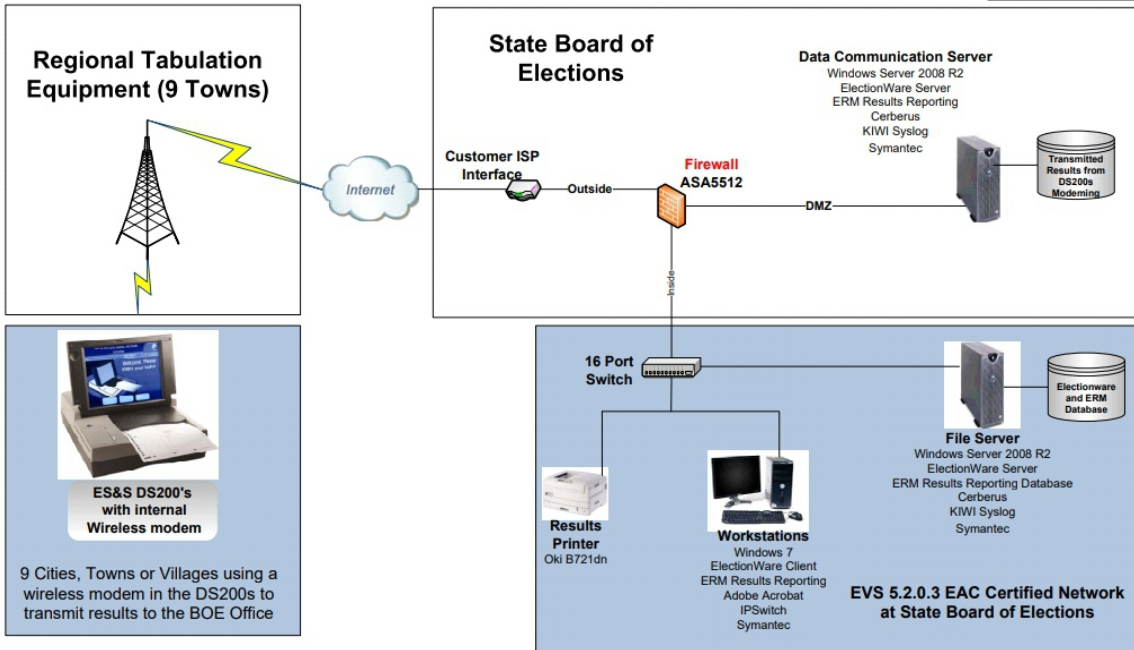
<sup>1</sup> <https://freespeechforpeople.org/wp-content/uploads/2020/01/EAC.ESS-Letter-re-modems-with-Attachments-01.07.20.pdf>

<sup>2</sup> Zetter, K. (2020). Election commission orders top voting machine vendor to correct misleading claims. <https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891>

**State of Rhode Island EVS 5.2.0.3/5.3.0.3  
 DS200 Modeming System Configuration**

October 23, 2015

Legend  
 EAC Certified Configuration  
 Extended Configuration



ES&S Contract AR2762 no. 30 Public Data Security<sup>1</sup>

3. **Public Data Transmission:** Contractor agrees that any and all transmission or exchange of system application data with the Eligible Users and State of Utah and/or any other parties expressly designated by the State of Utah, shall take place via secure means (ex. HTTPS or FTPS).
4. **Public Data Storage:** Contractor agrees that all Public Data will be stored and maintained in data centers in the United States. Contractor agrees that no Public Data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, except for devices that are used and kept only at Contractor's United States data centers, unless such medium is part of the Contractor's designated backup and recovery process. Contractor shall permit its employees and Subcontractors to access non-Public Data remotely only as required to provide technical support. Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited by this contract.
5. **Public Data Encryption:** Contractor agrees to store all data provided to Contractor, including State, as part of its designated backup and recovery process in encrypted form, using no less than 128 bit key and include all data as part of a designated backup and recovery process.
6. **Password Protection:** Contractor agrees that any portable or laptop computer that has access to the Eligible Users or State of Utah networks, or stores any Public Data is equipped with strong and secure password protection.



<sup>1</sup> AR2762 from Utah Department of Purchasing Division p. 23.

ES&S Contract AR2762 Attachment A

3. **Public Data Transmission:** Contractor agrees that any and all transmission or exchange of system application data with the Eligible Users and State of Utah and/or any other parties expressly designated by the State of Utah, shall take place via secure means (ex. HTTPS or FTPS).
4. **Public Data Storage:** Contractor agrees that all Public Data will be stored and maintained in data centers in the United States. Contractor agrees that no Public Data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, except for devices that are used and kept only at Contractor's United States data centers, unless such medium is part of the Contractor's designated backup and recovery process. Contractor shall permit its employees and Subcontractors to access non-Public Data remotely only as required to provide technical support. Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited by this contract.
5. **Public Data Encryption:** Contractor agrees to store all data provided to Contractor, including State, as part of its designated backup and recovery process in encrypted form, using no less than 128 bit key and include all data as part of a designated backup and recovery process.
6. **Password Protection:** Contractor agrees that any portable or laptop computer that has access to the Eligible Users or State of Utah networks, or stores any Public Data is equipped with strong and secure password protection.
7. **Public Data Re-Use:** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purpose enumerated in this Contract. Contractor further agrees that no Public Data of any kind shall be transmitted, exchanged, or otherwise passed to other Contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by the Eligible Users.
8. **Public Data Destruction:** The Contractor agrees that upon expiration or termination of this Contract it shall erase, destroy, and render unreadable all Public Data from all non-state computer systems and backups, and certify in writing that these actions have been completed within thirty (30) days of the expiration or termination of this Contract or within seven (7) days of the request of the Eligible User, whichever shall come first, unless the Eligible User provides Contractor with a written directive. It is understood by the parties that the Eligible User's written directive may request that certain data be preserved in accordance with applicable law.
9. **Services Shall Be Performed Within United States:** Contractor agrees that all of the Services related to Public Data that it provides to the Eligible Users will be performed by Contractor and Subcontractor(s) within the borders and jurisdiction of the United States.

## Utah Has Ability to Audit our Votes

Utah can do a full forensic audit on ES&S voting systems. “State of Utah or each County will be the sole owner and custodian of all election -related data in the ES&S system and will have.” ES&S states that the State of Utah or each County have “**unrestricted right to access and use this data without interference** by or assistance from vendor”.

- 2.15.1 Confirm that the State of Utah or County will be sole owner and custodian of all election-related data in the system purchased and must have the unrestricted right to access and use this data without interference by or assistance from vendor. ★

Text (Multi-Line)

-Yes, the State of Utah or each County will be the sole owner and custodian of all election-related data in the ES&S system and will have the unrestricted right to access and use this data without interference by or assistance from vendor. -Many ES&S state and county-level jurisdictions that program their own elections using the ES&S EMS. ES&S will provide training and extensive support through our technical support team. While the software is intuitive and easy to use, we ensure that assistance is available with phone or email support.



ES&S source code can be accessed by the State of Utah through the Escrow Contract as stated in both RFP Summary<sup>1</sup> and Contract AR2762 Attachment E<sup>2</sup>.

3.17.1 Describe your firm's Open Source Software (OSS) strategy. ★

4

Text (Multi-Line)

ES&S employs a disclosed source strategy by which interested parties, such as Independent Voting System Test Labs and the State & County Election Authorities, can review ES&S source code. ES&S believes this strategy balances the critical demands of both transparency and security. In addition, all executables and installation files are compiled in a trusted build environment by a third party. The third party then hashes all files and escrows them, along with the respective source code, to ensure field installations match the trusted builds identically.

---

Detailed Scope of Work for Contract #AR2762

Attachment : E

- The project milestones, tasks and deliverables will be detailed in the Project Plan and include a timeline of events.
- Disposal of old equipment
  - ES&S will provide a trade-in value for the old equipment (outlined in Attachment B) and dispose of old equipment on or before delivery of the new equipment.
- Maintenance and Support Plan selected by eligible user, with pricing outlined in Attachment B.
- Sole owner and custodian
  - The State of Utah or Eligible User will be sole owner and custodian of all election-related State of Utah or Eligible User data in the system purchased and must have the unrestricted right to access and use this data without interference by or assistance from ES&S.
- Escrow
  - ES&S maintains in escrow with Iron Mountain Intellectual Property Management, Inc., a copy of all program source code developed and used for our proprietary software and firmware, as well as any changes, modifications or updates to the source code.
  - Should ES&S cease operations and become unable to maintain and support proprietary software and firmware while under an obligation to do so, the State shall have the right to obtain the source code to the extent necessary to enable the State to use ES&S' proprietary software and firmware in accordance with the terms of the final contract to be mutually agreed upon by the parties.
  - The source code will remain the property of ES&S and may not otherwise be used by the State except as set forth in the escrow agreement.

---

<sup>1</sup> RFP Summary no. 2.15.16 from State Elections office GRAMA.

<sup>2</sup> AR2762 from Utah Department of Purchasing Division p 103.

## ES&S Contract AR2762 no. 61 Right to Audit<sup>1</sup>

### AR2762

R895 and correct any items that do not meet these guidelines at no cost to the agency; and Rule R895-14-1-4-2, which states that vendors proposing IT products and services shall provide Voluntary Product Accessibility Template® (VPAT™) documents. Contractor acknowledges that all Goods and Custom Deliverables that it licenses, contracts, or sells to DTS under this contract are accessible to people with disabilities.

- 61. RIGHT TO AUDIT:** Contractor agrees to, upon written request, permit Division, or a third party designated by the Division, to perform an assessment, audit, examination, or review of all of Contractor's sites and environments - including physical, technical, and virtual sites and environments - in order to confirm Contractor's compliance with this Contract; associated Scopes of Work; and applicable laws, regulations, and industry standards. Contractor shall fully cooperate with such assessment by providing access to knowledgeable personnel; physical premises; records; technical and physical infrastructures; and any other person, place, or object which may assist the Division or its designee in completing such assessment. In addition, upon request, Contractor shall provide the Division with the results of any audit performed by or on behalf of Contractor that would assist the Division or its designee in confirming Contractor's compliance with this Contract; associated Scopes of Work; and applicable laws, regulations, and industry standards.

### Attachment A

accessible to people with disabilities.

- 61. RIGHT TO AUDIT:** Contractor agrees to, upon written request, permit Division, or a third party designated by the Division, to perform an assessment, audit, examination, or review of all of Contractor's sites and environments - including physical, technical, and virtual sites and environments - in order to confirm Contractor's compliance with this Contract; associated Scopes of Work; and applicable laws, regulations, and industry standards. Contractor shall fully cooperate with such assessment by providing access to knowledgeable personnel; physical premises; records; technical and physical infrastructures; and any other person, place, or object which may assist the Division or its designee in completing such assessment. In addition, upon request, Contractor shall provide the Division with the results of any audit performed by or on behalf of Contractor that would assist the Division or its designee in confirming Contractor's compliance with this Contract; associated Scopes of Work; and applicable laws, regulations, and industry standards.

---

<sup>1</sup> AR2762 from Utah Department of Purchasing Division p 28.

# How does the EMS and VISTA work together?

“ElectionWare allows user to configure parameters and security settings.”<sup>1</sup> ES&S EMS exchanges information with VISTA, both importing and exporting.<sup>2</sup> The data is on removable USB thumb drives that are encrypted.

---

## Group 2.15: Election Management System

---

- 2.15.1 Provide a description of how your proposed system meets the ability to interface with Utah's existing statewide voter registration database (VISTA), including the ability to exchange data between the two systems. ★

Text (Multi-Line)

Our solution features robust import and export capabilities that would facilitate the exchange of data between VISTA and our EMS. We have worked with multiple customers to integrate with statewide systems and have considerable experience in this area. For example, in Michigan and Mississippi, we recently coordinated with those states to allow for (1) the importing of election data (contests, candidates, etc.) from their statewide system into Electionware, and (2) the exporting of results data from our EMS in the format required by their statewide system. Ultimately these efforts have resulted in increased efficiency, elimination of redundant data entry, and significantly increased the speed of results reporting statewide.

- 2.15. Provide a method for election configuration data to be securely transferred from the EMS to voting devices. ★

9

Text (Multi-Line)

-Electionware allows the user to configure parameters and security settings and create election media for the ExpressVote universal voting system, the DS200 central scanner and tabulator, and the DS850/DS450 central scanner and tabulators. -Electionware packages all needed data elements, including the election configuration, onto portable USB memory devices used to transfer the data to the voting devices and central tabulators. -To enhance security, the election definition cannot be modified once it is transferred to the proper system media. ES&S systems do not offer any data entry feature that can be used to alter programming. -Election definition files on removable USB memory devices are encrypted using military-grade encryption: FIPS-compliant Advanced Encryption Standard (AES) encryption using a certified library from RSA. ES&S employs strong AES-128 and AES-256 encryption to FIPS 140-2 standards using the RSA BSAFE Library with ECDSA (Certificate 1058).

- 2.15.1 Provide a method for securely receiving results and accumulating vote totals by precinct, district, jurisdiction and statewide. ★

0

Text (Multi-Line)

-On our tabulation devices, the results are saved to a USB memory device which is then uploaded into Election Reporting Manager (ERM) reporting software. -Files on the USB memory devices are digitally signed and encrypted using military-grade encryption. -ERM enables accumulation of vote totals in a variety of ways, including by precinct, district, jurisdiction, and statewide.

“All results are digitally signed and encrypted on the USB memory device in the DS200.”<sup>3</sup>

---

<sup>1</sup> 2018 WA17018 RFP Summary, Utah Elections Office GRAMA, 33

<sup>2</sup> 2018 WA17018 RFP Summary, Utah Elections Office GRAMA, p 30

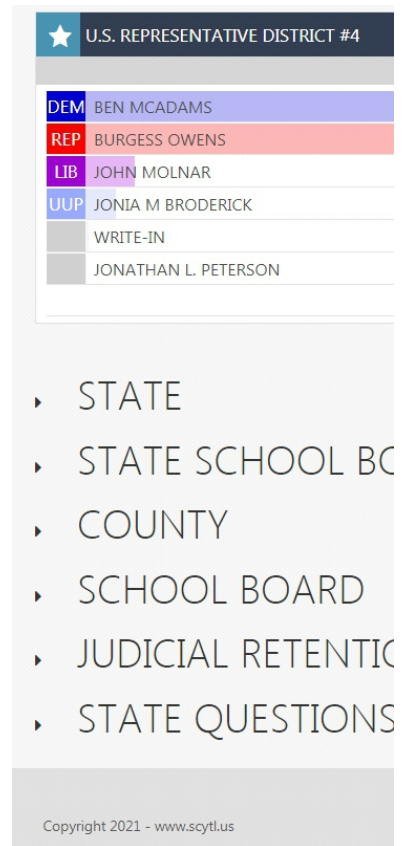
<sup>3</sup> 2018 WA17018 RFP Summary, Utah Elections Office GRAMA, p 37

2.16.1 Provide a description of how the proposed system provides a secure means to upload vote count results to the EMS. ★

Text (Multi-Line)

-All results are digitally signed and encrypted on the USB memory device in the DS200. After the polls close, poll workers may remove the system's USB flash drive containing the unit's election results and securely transport the election media to the voting EMS at Election Central. -The DS850/DS450 central count scanners transmit results data by writing encrypted, digitally signed data to a USB media device. Results on the USB memory devices are then uploaded to Election Reporting Manager (ERM).

The encryption is to secure the votes when transmitted in reporting software. Exhibit 21 in *Feehan v. Wisconsin Elections Commission*, the affidavit explains the use of COTS, encryption, and reporting software Scytl to cleanse and shuffle the votes and explains how an algorithm could be used to redistribute the votes.<sup>1</sup> The Associated Press uses Scytl. Salt Lake County uses Scytl, too. On the Salt Lake County 2020 Elections results found here: [https://results.enr.clarityelections.com/UT/Salt\\_Lake/107137/Web02.262834/#/](https://results.enr.clarityelections.com/UT/Salt_Lake/107137/Web02.262834/#/), scroll to the bottom and it will say copyright of Scytl.



<sup>1</sup> Wisconsin District Court. (2020). *Feehan v. Wisconsin Elections Commission, Exhibit 21*. <https://www.courtlistener.com/docket/18702085/1/21/feehan-v-wisconsin-elections-commission/>

**Intelligence X**  
shows dark web results of

- Employee Credentials
- 12 Username and Password combinations

Popular dark web searches publicly reveal the authorization credentials of Dominion Voting employees.

**ELECTION Systems & Software**  
provides services for

**DOMINION VOTING**

**Data collectors, election monitors, and research firms**

Outfits that watch vote numbers and trends to figure out how elections are going

**Decision Desk HQ**

Four-year old Washington DC company responsible for calling the race before all the votes are tallied

CNN and other mainstream outlets that favor Joe Biden quickly announce Decision Desk's results and run with it as if it was official

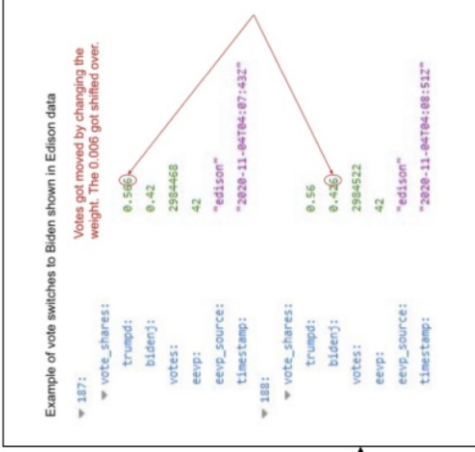


Physical Ballots are converted to digital images via ImageCast



An array of techniques are deployed to switch Trump votes into Biden votes or to delete Trump votes.

Edison Research published unedited data which shows anomalies indicative of voter fraud



Votes as percentages allow for small decimal shifts to move large amounts of votes from Trump to Biden.

Votes were being represented as percentages of all votes instead of simply counting every vote.

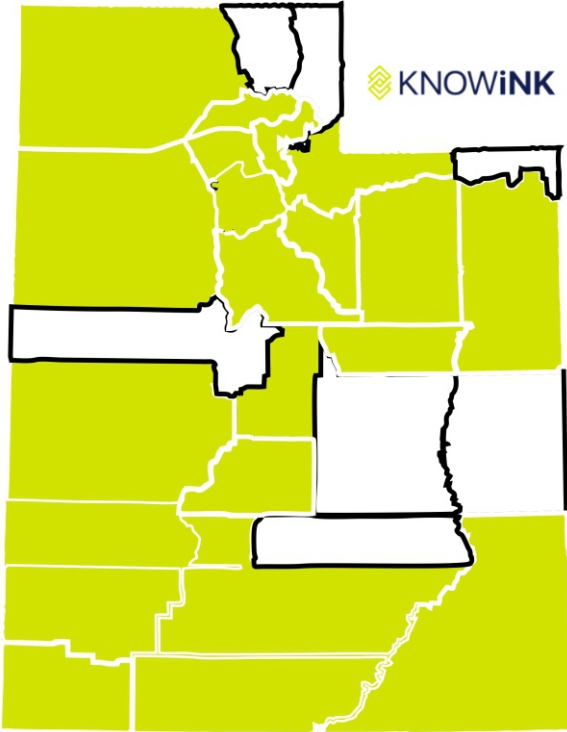
```

HOW VOTES ARE STORED IN DOMINION
{
  "Trump": "0.5407",
  "Biden": "0.4587",
  "VoteCount": "98098"
}

HOW IT WOULD BE HONESTLY STORED
{
  "Trump": "7878734",
  "Biden": "9809823"
}

```

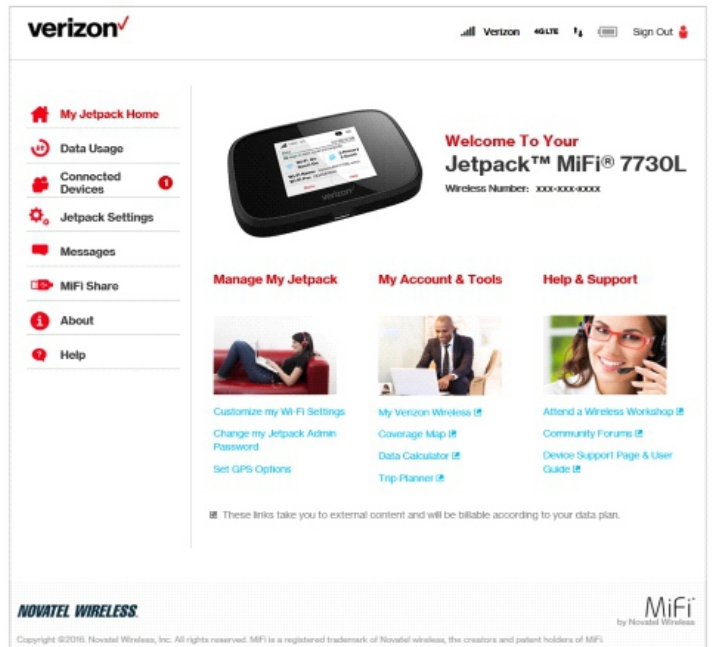
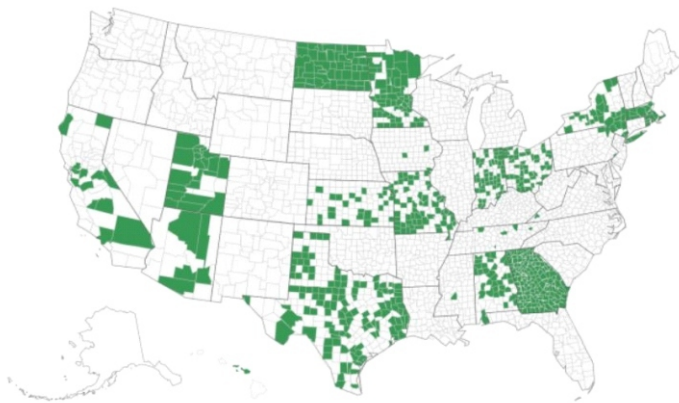
KNOWiNK Poll Pads are used to live sync with Utah's VISTA voter registration.



VSM in Utah (varies by county)

- Poll Pad Apple iPad WiFi 32 GB
- Poll Print Tablet Apple iPad 23GB MR/FLL/A SpaceGrey
- Poll Print Software v.2
- iSync Drive 8 GB
- Green MiFi Lightening Cable
- USB wall charger 2.4/5V
- I360 stand
- Stylus
- Transport Case
- MDM Enrollment
- Basic Poll Manager
- Live Syncing & Basic Poll Manager
- Verizon Jetpack Novatel MiFi 7730L
- Verizon Wireless Data Plan
- Meraki MR42
- Meraki Networking Package
- Star Micronics Bluetooth Receipt Printer
- OKI C712dh Color Laser Printer w/19" Tray
- Star Micronics Power Supply PS604A - 24B1
- Poll Print Cabinet w/battery backup
- Poll Print Package (Belkin Ethernet Adapter, Mikrotek Router, Ethernet Cables)
- Nanuk 920 Case (receipt printer, foam)
- ePulse Connectivity Software
- ePulse Track - Asset & Inventory Software
- UT VR (VISA) Integration
- Poll Print Software
- Encoder Voter Access
- Barcode Service
- CheckPoint Help Desk & Issue Tracking Software
- iTrack Asset and Inventory Software

KNOWiNK Poll Pad usage in November 2020 (click map for details)



With reports of voter database registration infiltration/breach in 2020 November election, which is suspected of being used to correct phantom voters, KNOWiNK needs to be audited to ensure election security.<sup>1</sup> KNOWiNK had issues in 2019 Philadelphia election with “failure to properly connect to voting machine printers and inadequate election night reporting”. Philadelphia had no confidence in using KNOWiNK for 2020 elections.<sup>2</sup> These issues with poll pads happened throughout the country. Another concern is using the pollbooks to access voting machines.<sup>3</sup> KNOWink Poll Pads use a Verizon JetPack Novatel MiFi 7730L, a Verizon WiFi hotspot for live syncing to VISTA, Utah’s voter registration database. This requires a Verizon Wireless Data Plan.

- 4.4.6** If the EPB hardware is available from COTS sources, please indicate purchasing sources. If the software is not available from COTS sources, respond with "N/A."

Text (Multi-Line)

The EPB hardware is available from COTS sources, with the following purchasing sources: - Apple iPad: Any Apple certified distributor or reseller. - Meraki Access Point: Any certified Cisco distributor. - Hotspots: KNOWiNK has a partnership with Verizon, but any cellular provider deemed sufficient by the jurisdiction will be accommodated. The EPB software is proprietary - N/A.

- 4.4.7** Describe the capabilities of an EPB, including: (a) ability to electronically list, search, identify, and authenticate eligible voters, (b) ability to interface with Utah's existing statewide voter registration database (VISTA), (c) ability to electronically capture voter signatures, (d) customization options.

Text (Multi-Line)

a. Each EPB will contain the jurisdiction’s database of registered voters. Each EPB will allow for the scanning of a Driver’s License or State Voter ID Card as a search function, which will quickly and efficiently locate the voter record. Alternatively, a manual search can be performed, using the first 3 letters of the voters first name, and last name. Voter can then be selected, and each voter record will display the information relevant to verifying individual voter’s eligibility, including any voter statuses supplied by VISTA. Customized procedural guidance for the poll workers can be set to prompt the specific processes associated with the voters’ statuses. b. KNOWiNK can interface with VISTA per the needs and requirements of the State of Utah. They can develop a live connection via API to the VISTA registration database, if desired, for which they would employ a live data sharing agreement. The Poll Pad solution is already configured to accept a traditional data file from VISTA. c. KNOWiNK utilizes the iPad’s Capacitive Touchscreen and stylus to capture a voter signature during the check-in process. Each signature is archived and can be extracted for verification or upload back into the VISTA system. d. Poll Pad is designed to be a highly customizable solution. KNOWiNK deploys EPB’s in more jurisdictions across more states than any other vendor. This extensive experience equates to their effective, customizable platform and the ability to quickly adapt the solution software to fit a jurisdiction’s unique needs and requirements.

---

<sup>1</sup> <https://electionwiz.com/2021/07/07/update-letter-reportedly-sent-to-voters-says-maricopa-county-voter-information-was-hacked-during-2020-election/>

<sup>2</sup> Lai, J. *Philadelphia Says New Electronic Poll Books Don’t Work*. The Philadelphia Inquirer.

<sup>3</sup> Zetter, K. (2020). The election security hole everyone ignores. Politico.

- 4.4.6 If the EPB hardware is available from COTS sources, please indicate purchasing sources. If the software is not available from COTS sources, respond with "N/A."

Text (Multi-Line)

The EPB hardware is available from COTS sources, with the following purchasing sources: - Apple iPad: Any Apple certified distributor or reseller. - Meraki Access Point: Any certified Cisco distributor. - Hotspots: KNOWiNK has a partnership with Verizon, but any cellular provider deemed sufficient by the jurisdiction will be accommodated. The EPB software is proprietary - N/A.

- 4.4.7 Describe the capabilities of an EPB, including: (a) ability to electronically list, search, identify, and authenticate eligible voters, (b) ability to interface with Utah's existing statewide voter registration database (VISTA), (c) ability to electronically capture voter signatures, (d) customization options.

Text (Multi-Line)

a. Each EPB will contain the jurisdiction's database of registered voters. Each EPB will allow for the scanning of a Driver's License or State Voter ID Card as a search function, which will quickly and efficiently locate the voter record. Alternatively, a manual search can be performed, using the first 3 letters of the voters first name, and last name. Voter can then be selected, and each voter record will display the information relevant to verifying individual voter's eligibility, including any voter statuses supplied by VISTA. Customized procedural guidance for the poll workers can be set to prompt the specific processes associated with the voters' statuses. b. KNOWiNK can interface with VISTA per the needs and requirements of the State of Utah. They can develop a live connection via API to the VISTA registration database, if desired, for which they would employ a live data sharing agreement. The Poll Pad solution is already configured to accept a traditional data file from VISTA. c. KNOWiNK utilizes the iPad's Capacitive Touchscreen and stylus to capture a voter signature during the check-in process. Each signature is archived and can be extracted for verification or upload back into the VISTA system. d. Poll Pad is designed to be a highly customizable solution. KNOWiNK deploys EPB's in more jurisdictions across more states than any other vendor. This extensive experience equates to their effective, customizable platform and the ability to quickly adapt the solution software to fit a jurisdiction's unique needs and requirements.

FILE FROM STATE ELECTIONS GRAMA: Dominion Voting Systems Inc\_Redacted

- 4.4.6 If the EPB hardware is available from COTS sources, please indicate purchasing sources. If the software is not available from COTS sources, respond with "N/A."

Text (Multi-Line)

The EPB hardware is available from COTS sources, with the following purchasing sources: - Apple iPad: Any Apple certified distributor or reseller. - Meraki Access Point: Any certified Cisco distributor. - Hotspots: KNOWiNK has a partnership with Verizon, but any cellular provider deemed sufficient by the jurisdiction will be accommodated. The EPB software is proprietary - N/A.

**"EPB will contain jurisdiction's database of registered voters."**

**"KNOWiNK can interface with VISTA per the needs and requirements of the State of Utah. They can develop a live connection via API to the VISTA registration database."**

**"live data sharing agreement"**

**"Upon import of the voter file from VISTA, the Poll Pad solution will map each voter to their associated voter status."**

- 4.4.7 Describe the capabilities of an EPB, including: (a) ability to electronically list, search, identify, and authenticate eligible voters, (b) ability to interface with Utah's existing statewide voter registration database (VISTA), (c) ability to electronically capture voter signatures, (d) customization options.

Text (Multi-Line)

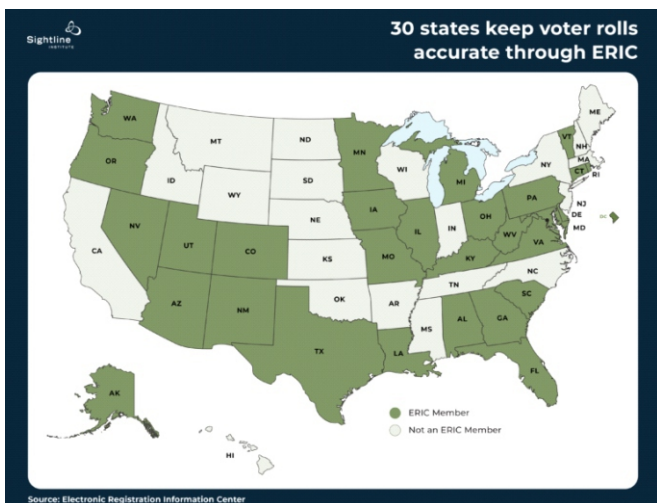
a. Each EPB will contain the jurisdiction's database of registered voters. Each EPB will allow for the scanning of a Driver's License or State Voter ID Card as a search function, which will quickly and efficiently locate the voter record. Alternatively, a manual search can be performed, using the first 3 letters of the voters first name, and last name. Voter can then be selected, and each voter record will display the information relevant to verifying individual voter's eligibility, including any voter statuses supplied by VISTA. Customized procedural guidance for the poll workers can be set to prompt the specific processes associated with the voters' statuses. b. KNOWiNK can interface with VISTA per the needs and requirements of the State of Utah. They can develop a live connection via API to the VISTA registration database, if desired, for which they would employ a live data sharing agreement. The Poll Pad solution is already configured to accept a traditional data file from VISTA. c. KNOWiNK utilizes the iPad's Capacitive Touchscreen and stylus to capture a voter signature during the check-in process. Each signature is archived and can be extracted for verification or upload back into the VISTA system. d. Poll Pad is designed to be a highly customizable solution. KNOWiNK deploys EPB's in more jurisdictions across more states than any other vendor. This extensive experience equates to their effective, customizable platform and the ability to quickly adapt the solution software to fit a jurisdiction's unique needs and requirements.

FILE FROM STATE ELECTIONS GRAMA: Dominion Voting Systems Inc\_Redacted



# Utah Voter Registration: ERIC (Elections Registration Information Center)

ERIC founded 2012  
with Brennan Center  
For Justice PEW  
Grant



Funded by:



Who has access to ERIC:  
Lt Governor's Election Office  
Driver's License Division  
County Clerk  
Department of Health  
US Postal Service

## Who Pays For ERIC Operations?

The member states. Each state pays annual dues, which are determined by a formula approved by the ERIC membership. The formula includes citizen voting age population as a factor. Large states pay more than small states. The annual budget for FY 2019-20 is approximately \$947,000.



**Vox**  
**Election officials are scrambling to get their cut of Mark Zuckerberg's \$250 million**

Theodore Schleifer · 10/7/2020

Like Comments



© Paul Marotta / Getty Images Mark Zuckerberg's donation has led to a gold rush for his cash.

Mark Zuckerberg's \$250 million gift to bolster local governments has set off a gold rush across the country as frenzied election officials rush to apply, secure, and deploy the money.

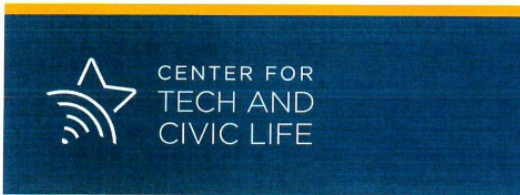
Tuesday, December 15, 2020 at 13:12:13 Mountain Standard Time

**Subject:** Your payment from The Center for Technology and Civic Life is on its way!  
**Date:** Wednesday, September 30, 2020 at 1:01:50 AM Mountain Daylight Time  
**From:** Bill.com Operations  
**To:** Justin Anderson

**The Center for Technology and Civic Life**

Hi Utah County Government,

The check will arrive around 10/06/20. This date is an estimate based on USPS delivery speed. The payment is for these invoices:



Invoice #	Due Date	Amount	Payment Amount
Utah County Government	09/29/20	\$241,664.50	\$241,664.50
<b>Total:</b>			<b>\$241,664.50</b>

October 9, 2020

Cache County, Utah  
 Cache County Government  
 179 N Main Street, Suite 102  
 Logan, Utah 84321

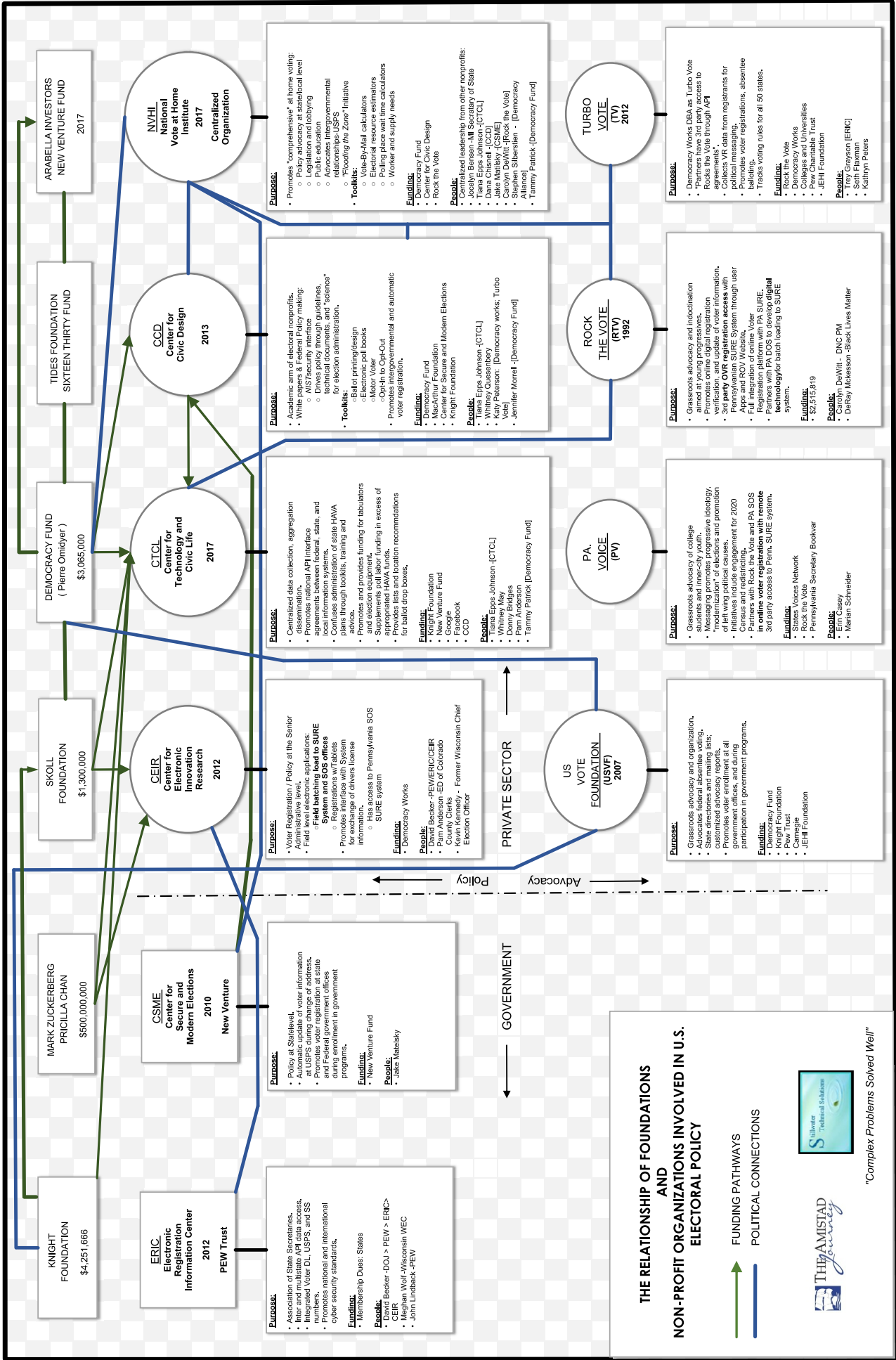
Cache County Government:

I am pleased to inform you that based on and in reliance upon the information and materials provided by Cache County, the Center for Tech and Civic Life ("CTCL"), a nonprofit organization tax-exempt under Internal Revenue Code ("IRC") section 501(c)(3), has decided to award a grant to support the work of Cache County ("Grantee").

The following is a description of the grant:

**AMOUNT OF GRANT:** \$53,945.50 USD

**PURPOSE:** The grant funds must be used exclusively for the public purpose of planning and operationalizing safe and secure election administration in Cache County in 2020 ("Purpose").



"Complex Problems Solved Well!"