All political power is vested in and derived from the people; all government, of right, originates from the people, is founded upon their will only, and is instituted solely for the good of the whole.

Constitution of the State of Colorado, Article II (Bill of Rights), Section 1
Team Intro

• U.S. Election Integrity Project
  Grassroots, multiple states, hundreds of citizens

• Our Objectives:
  
  CONNECT: Enable election integrity groups, efforts, and resources

  FIND THE TRUTH: What’s REALLY true regarding our elections and systems

  SHARE THE TRUTH: Share the truth with citizens and public officials

  RESTORE ELECTION INTEGRITY: Restore confidence in Colorado elections
What are we going to talk about today?

1. **What we have:** Colorado’s election systems

2. **What we know:** Serious vulnerabilities in CO systems - NOT secure, NOT securable

3. **What we don’t know:** Magnitude of compromise & exploitation, by whom

4. **What we’ve seen:** *Smoke* – Significant unexplained indications in CO elections

5. **What must be investigated:** We *MUST investigate* to find or rule out fire

6. **What must be done:** Restore integrity & trust – spread the truth and...

---

**FIX THE SYSTEM**
Why We’re Here

**Voters want free and fair elections**

How likely is it cheating affected the outcome of the 2020 Presidential Election?

"**LIKELY YES**"
- 74% of Republicans
- 30% of Democrats
- 50% of UAF

What’s more important: integrity or voting ease?

"**INTEGRITY**" 60% of voters (majorities in all racial groups)

**Voters don’t trust the system**

**CO voters level of trust in our institutions?**

- Federal Gov: 65%
- State Gov: 54%
- Local Gov: 55%
- National Media: 67%
- Local Media: 59%

**Republican voters feel wronged**

**CO Republican voters think:**

“The government is rigged and run by liberal bureaucrats who stole the election.”
20 Years of “Efficiency” & “Accessibility”  
...rather than Integrity  

2002  

2009  
HB1018: Statewide Voter Registration System – out of county hands; centralized vulnerability  
HB1205: Internet-Based Voting (Pilot) – the camel’s nose under the tent flap  
HB1216: Permanent Mail in Voting – “convenience” over ballot chain of custody and integrity

2013  
HB1303: Voter Access and Modernized Elections Act

2018  
SB150: Voter Registration Individuals Criminal Justice System  
SB233: Elections Clean-up

2019  
HB1266: Restore Voting Rights Parolees  
SB235: Automatic Voter Registration – bloated voter rolls to complement mail-in voting

2020  
HB1149: 16-year-olds Voting in School District Elections (In Committee)  
Proposition 113: National Popular Vote Interstate Compact Referendum – subversion of the electoral college

2021  
HB1086: Proof of Citizenship (Deferred)  
SB177: Foreign-influence In Politics
What We Have

The processes, systems and tools in Colorado elections.
CO Elections

What We Have

Either:

• Our current system is immaculate: “The Gold Standard!”
• Or voters have good reason to distrust state government

It ISN’T because some legislators tried to do something about election integrity.

It’s because the Emperor has No Clothes
What We Have

CO Elections – The Narrative Begins...

SCORE: Statewide Voter Registration System
- SOS maintained and hosted software and hardware
- Internet connected devices required for updating voter information in real time

Life of a Mail Ballot
- BALLOT CONTENT: Contents are printed, registered SOS and administered
- BALLOT PACKET MAILED: 20 days before the election
- BALLOT PICK UP: Ballots are mailed and received from counties
- VOTING: Voter receives ballot, signs it and returns it
- BALLOT SORTING: County maintains and provides the signature canvas
- BALLOT REVIEW: Ballots are opened by a neutral third party
- ENVELOPE OPENING: Ballots are opened by third party and sent to county
- COUNTING & DUPlication: Ballots are counted and sent to central count server
- 8 DAYS POST ELECTION: Final results are certified and released to the public
- BALLOT RESULTS: Results are posted online and published

Election Management System (Dominion)
- County maintained software and hardware
- NCN internet connected county owned devices connected to a central count server located in the same room
- Election Night Reporting Website
- Scytl maintained and hosted software and hardware, SOS licensed administrator
- Internet connected county owned devices required for presenting results to the public
What We Have

CO Elections – A Systems Perspective

2,676 pieces of SoS-certified voting equipment
What We Have

CO Elections – Reasonable Questions

**Ballot Content**
- Voting system election event designer controlled by?
- SCORE upload accessible by?
- Print companies secure ballot .PDF

**Ballot Pickup**
- “Bipartisan” or “multipartisan?” e.g. “Democrat” & Social Democrat
- “Secure?”

**Ballot Packed Mailed**
- USPS tracking?
- BallotTrax tracking?
- # Undeliverable?
- # In wrong hands?

**Voting**
- # Printed by print vendors AND?
- # Marked by machine AND?
- # Signatures forged / machine
- # Printed on envelopes?

**Return Ballot**
- “Secure?”
- Video ever reviewed?
- What security with the USPS?
What We Have

CO Elections – Reasonable Questions

Signature Verification
- # Signatures in SCORE per voter? From?
- How many rejected this vs. last election vs. last?
- By cert. doc examiners, comp systems or volunteers?

Counting & Duplication
- Duplication BEFORE counting?
- Is adjudication a software application, a procedure, or a function?

Envelope Opening
- Last chance to reject a ballot from an ineligible voter?
- No count of envelopes versus ballots

Audit / Certification
- Voting system election event designer controlled by?
- SCORE upload accessible by?
- Print companies secure ballot .PDF?
CO Elections – Reasonable Questions

What We Have

Adversary Tactics
- Reconnaissance
- Resource dev
- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- C2
- Exfiltration
- Impact
- Network effects
- Remote service
- Impacts

Initial Access
- Drive-by Compromise
- Exploit public facing application
- External remote services
- Hardware additions
- Phishing
- Replication through removable media
- Supply chain compromise
- Trusted relationship
- Valid accounts

WebSCORE connects through the INTERNET?
How many web pages, servers, and orgs connect to SCORE?

Election Management System (Dominion)
"County Maintained software and hardware?
CAN THEY:
- Audit it?
- Update it?
- Use their own USB memory?

Election Night Reporting Website
Where does our election data go?
Scytl: Spain, private Owns SOE; together largest election provider in the U.S. zero outside security evaluation
# What We Have

## CO Elections – Registration Systems

<table>
<thead>
<tr>
<th><strong>SCORE</strong></th>
<th><strong>SABER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statewide</strong></td>
<td><strong>“security testing” wasn’t; it was functional testing</strong></td>
</tr>
<tr>
<td><strong>Colorado</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Registration &amp; Election system</strong></td>
<td></td>
</tr>
</tbody>
</table>

- 2008
  - Registered voter database
  - Signature repository
  - Ballot tracking
  - EPollbook *HP/SABER Corp base code (Electus)*

- Testing lead-listed tech skills:
- “MS Office, scanner/printer setup”
- SABER “security” devices are compromised (150+ known vuls)
- **No 24/7 monitoring/defense;** SCORE/webSCORE (ePollbook) are ONLINE: https://score.sos.colorado.gov/logon/LogonPoint/tmindex.html
CO Elections – Registration Systems

- **Kansas Crosscheck** – free multi-state voter registration data sharing
  - Focused on reduction of duplicate registrations, dead voters
  - CO SoS withdrew CO in Jan ’19; ACLU Dec ’19 suit halted program

- **Electronic Registration Information Center (ERIC)** – formed 2012
  - Non-profit org (w/Pew funds), but charged CO $25k + annual dues
  - CO obliged to give DMV data – focused on maxing out voter rolls

- **ERIC states** - 4.2x new voter registrations of non-ERIC states
What We Have

CO Elections – Ballot Tracking & Curing

• **BallotTrax**
  - Given CO voter/ballot info by SoS, regardless of citizen opt-in
  - No CO or independent security or auditing of any kind
  - “Our product does not require federal or state certification”

• **TXT2CURE**
  - “Patented and Proprietary security process” – we have NO INSIGHT, whatsoever
  - “Text ‘Colorado’ to 2VOTE, click on link, Enter Voter ID (157272X)
  - “Affirm” ballot return
  - Sign affidavit on phone
  - Take photo of acceptable ID, and submit
What We Have

CO Elections – Voting Systems

• **Dominion Voting Systems (DVS) Democracy Suite (DS) 5.11CO**
  • Used in 20 U.S. states, 62 CO Counties
  • Consists of (Dell “Commercial-Off-The-Shelf (COTS) + tablets + scanners):
    • Election Management System (EMS) – tallies cast vote records (CVR) from ICC; reports; supports election event design (ballots, etc)
    • ImageCast Central (ICC) - scanner/tabulation
    • Adjudication System Server/Client (can also be run on EMS or ICC) - modifying ballots
    • ImageCast X – ballot marking device for voter assistance
    • ImageCast Voter Activation (ICVA) – programming cards for use in ICX
CO Elections – Voting Systems

• **Clear Ballot ClearVote 2.1**
  - Used in 6 states, 2 CO counties: Garfield, Douglas - ~7% of CO pop.
  - Consists of:
    - ClearAccess – Ballot Marking Device - Dell “COTS,” touchscreens, printers
    - ClearCount – “Browser-based” scanner/tabulation – Dell “COTS,” scanners
    - ClearDesign – Election designer – Dell “COTS”

• **Uniformed And Overseas Citizens Absentee Voting Act (UOCAVA)**
  - Mailed ballots & blank ballot .pdf sent by email
  - Returned via email (printed, signed, scanned) or fax (waives right to secrecy)
What We Have

CO Elections – Audit System

• **Colorado RLA (CORLA) Tool, based on DemocracyWorks-led software**
  - “Seed” selected with roll of 10-sided dice, on video
  - Software “randomly” (opaquely) selects “efficient” number of ballots to audit
  - DemocracyWorks = Democracy Fund/Alliance; Bridge Alliance; OpenSocieties

• https://www.randomlists.com/random-numbers
What We Have

CO Elections – The Narrative Continues...

• “Colorado is the ‘Gold Standard’ of safe and secure voting” – Gov. Polis
• “Colorado’s election model is the nation’s gold standard” – SecState Griswold
• “...arguably the best system in the country.” – ELP CCR Broerman
• “Our votes are not being manipulated” – Congressman Ken Buck
• “There’s no evidence” – CO Rep Fields
• “Dominion...tested(RLA) in 62 (CO) counties at least 807 times.” – fmr SoS Williams
• “No voting systems connected to the internet” – Nobody who has checked
• “No election fraud has been proven in court” – The Media
What We Know

There are significant system vulnerabilities - they are NOT secure nor securable.
WHEN YOUR ELECTION SYSTEMS AREN’T SECURE.

Their Control

Your “Controls”
What We Know

CO Elections — Process Vulnerabilities

• **Voter registration safeguards are weak:**
  - No in-person verification for massive number of registered voters
  - ID requirements ridiculously lax
  - Tens of thousands of ballots undeliverable — how accurate can SCORE be?

• **ERIC makes registration worse:**
  - In 2012 ERIC contacted 723k “eligible individuals” in Colorado, but only 10% registered, and less than half of those voted

• **Initial and recurring cybersecurity vulnerability assessment is completely inadequate:**
  - No supply chain security
  - No apparent concept of threat-level
  - Focus on “disinformation” instead of cybersecurity
What We Know

CO Elections – Physical Vulnerabilities

4 Seconds

30 Seconds

4 Seconds
What We Know

CO Elections – Systems Vulnerabilities (1/10)

• U.S. Elections are the biggest cybersecurity target in the world **No prize is worth more**

• Are voting systems connected to the Internet? **Yes.** WiFi verified in at least Georgia and Arizona

• Security OR anonymity - cannot have security AND anonymity

• The engineering of our election systems is insufficient
  • Requirements must be testable and verifiable
    • Commercial systems compete on features and performance
  • But mission critical systems **must not fail**

• Voting systems should be treated as mission critical systems
  • Below engineering for deep space missions – which can endanger 10s of people
  • Well below engineering for human flight – which can endanger 100s of people
  • Voting systems affect the entire population (~330 million)

• EAC Certifications granted despite known VVSG violations
What We Know

CO Elections – Systems Vulnerabilities (2/10)

Dominion Specifics:

• Millions of line of C/C++ will have memory leak(s)
  ALWAYS security exposures
• Coding conventions extremely lax
• Version 4 (@sec) was certified despite:
  • Encryption key violations (hard-coded, unencrypted on disk, weak selections)
  • Mixed-mode arithmetic
  • Complex branching – reviewer admitted couldn’t tell if there was a problem
  • Privilege escalation – means a perpetrator would “own” the machine
• Version 5 (Pro V&V “tested”)
  • Only documented code review done via automated tools - only enforce convention/best practices – CAN’T find security risks directly
  • Certified despite known SQL injection exposure
• It is questionable whether problems are ever fixed after certification
## What We Know

### CO Elections – Systems Vulnerabilities (3/10)

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11CO (EMS) Election Management System</td>
<td>MS Windows Server 2016</td>
<td>S</td>
<td>19+</td>
</tr>
<tr>
<td></td>
<td>Election Event Designer (EED)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Results Tally and Reporting (RTR)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>File System Service (FSS)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Audio Studio (AS)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Data Center Manager (DCM)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Election Data Translator (EDT)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Application Server (APPS)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Adjudication Services</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Adjudication Client</td>
<td>S</td>
<td>Proprietary</td>
</tr>
</tbody>
</table>
## CO Elections – Systems Vulnerabilities (4/10)

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11 CO (EMS) - CTD</td>
<td>DVS SmartCard Helper Service</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Election Management System</td>
<td>ImageCast Voter Activation (ICVA)</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Dell PowerEdge R630 (EMS Server)</td>
<td></td>
<td>H</td>
<td>17+</td>
</tr>
<tr>
<td>Dell Precision T3420 (Client/Server)</td>
<td></td>
<td>H</td>
<td>36+</td>
</tr>
<tr>
<td>Dell Precision T1700 (Server)</td>
<td></td>
<td>H</td>
<td>2+</td>
</tr>
<tr>
<td>Dell PowerEdge R710 (EMS Server)</td>
<td></td>
<td>H</td>
<td>2+</td>
</tr>
<tr>
<td>Dell PowerEdge T630 (EMS Server)</td>
<td></td>
<td>H</td>
<td>2+</td>
</tr>
<tr>
<td>Election Data Exchange Station (EDES)</td>
<td></td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Dallas 1-wire device driver</td>
<td></td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>Cepstral Voices</td>
<td></td>
<td>S</td>
<td></td>
</tr>
</tbody>
</table>
## What We Know

### CO Elections – Systems Vulnerabilities (5/10)

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11CO (EMS) - CTD</td>
<td>Election Management System</td>
<td>S</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>MS SQL Server Standard</td>
<td>S</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>MS Visual J# 2.0</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>RAID Utility</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maxim iButton</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ACS ACR39U Smart Card Reader</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apacer, Centon USB stick</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>UPS Drivers</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>DVS DS 5.11CO (ICC)</td>
<td>ImageCast Central</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dell Optiplex 9030 AIO</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Dell Optiiplex 3050 AIO</td>
<td>H</td>
<td>1</td>
</tr>
</tbody>
</table>
What We Know

CO Elections – Systems Vulnerabilities (6/10)

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11CO (ICC) - CTD ImageCast Central</td>
<td>Dell Optiplex 7440 AIO</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Dell Optiplex 7440 AIO</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Dell Optiplex 7050</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Canon DR-G1130 Scanner</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Canon DR-M160II Scanner</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interscan HiPro 821dd Scanner</td>
<td>H</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Canon DR-X10C Scanner</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uninterruptible Power Supply</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router</td>
<td>H</td>
<td></td>
</tr>
</tbody>
</table>
## CO Elections – Systems Vulnerabilities (7/10)

What We Know

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11CO (ICC) - CTD ImageCast Central</td>
<td>Web Server</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICC Application</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Adjudication Client</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>MS Windows 10</td>
<td>S</td>
<td>1100+</td>
</tr>
<tr>
<td></td>
<td>Kofax Scanning</td>
<td>S</td>
<td>* (Active-X)</td>
</tr>
<tr>
<td></td>
<td>MS Visual C++ 2015</td>
<td>S</td>
<td>1 (WIX Toolset)</td>
</tr>
<tr>
<td></td>
<td>Canon Scanner Drivers</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>DVS DS 5.11CO (ICX) ImageCast X</td>
<td>aValue 21.5&quot;</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Samsung Galaxy Note Pro</td>
<td>H</td>
<td></td>
</tr>
</tbody>
</table>
## What We Know

### CO Elections – Systems Vulnerabilities (8/10)

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/ S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11CO (ICX) - CTD ImageCast X</td>
<td>Samsung Galaxy Tab</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KFI VRP3</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lavalink STS-2UE Hub</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apacer, Centon, Apricorn USB sticks</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ACOS-6-64 Smart Cards</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP M402dne Laser Printer</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Android 8.1 (Avalue)</td>
<td>S</td>
<td>254</td>
</tr>
<tr>
<td></td>
<td>Android 4.4.2 (Galaxy Tab)</td>
<td>S</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td>Android 5.0.2 (Galaxy Tab)</td>
<td>S</td>
<td>183</td>
</tr>
<tr>
<td></td>
<td>Sip &amp; Puff Enabling Device #972</td>
<td>H</td>
<td></td>
</tr>
</tbody>
</table>
## What We Know

### CO Elections – Systems Vulnerabilities (9/10)

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>H/S</th>
<th>KNOWN VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS DS 5.11CO (ICX) - CTD ImageCast X</td>
<td>Paddle Switches #971</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paddle Switches AbleNet 10033400</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td>DVS DS 5.11CO (ICVA) ImageCast Voter Activation</td>
<td>Dell Latitude 3480</td>
<td>H</td>
<td>1+</td>
</tr>
<tr>
<td></td>
<td>ICVA App</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td>Smart Card driver</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DVS Smart Card Helper</td>
<td>S</td>
<td>Proprietary</td>
</tr>
<tr>
<td>CBG CV 2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO RLA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCORE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TXT2Cure</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CO Elections – Systems Vulnerabilities (10/10)

- **El Paso County** - Dell Precision T3420, DS EMS Server, Serial: FZTQCH2 (30+)
- **From Dell:**
  - Warranty expired 30 March 2020
  - Built with Intel 8260/7265/3165 WiFi Driver
  - **URGENT – DSA-2020-059** “local authenticated malicious user w/low privileges could exploit this vulnerability to gain unauthorized access on the root”
  - Thunderbolt Driver/Controller
  - Command Update App – “multiple arbitrary file deletion vulnerabilities”
  - Intel Ready Mode Technology Application – Remote sysadmin
  - Dell WatchDog BIOS/Driver user interface
  - Dell Command Intel vPro Out-of-Band “remotely manage client systems regardless of system power state”
What We Know

Threat and Vulnerability Indicators (1/2)

- **2008** — Credit card fraud specialist: “man-in-the-middle” attack used to rig 2004 election
- **2009** — Stuxnet virus spreads via USB, encrypted zero-day exploit, & spoofed driver cert
- **2014** — Red Team report on DVS DS 4.14-A: 7 “High Severity” security findings
- **2015** — U.S. DoD Joint Staff unclassified net hacked; APT29 – 2 weeks to fix
- **2018** — Oct, PRC supply chain motherboard chip attack vs. Apple/Amazon/et al, via
- **2019** — CA Report on DVS DS 5.10: “issues...(re:)
  - Audit logging, passwords, anti-virus, and installation
  - Technician keys contain all the same default passcode
  - Security seals, locks and security screws can be circumvented,” EMS Server “…only able to detect and clean one of…four (virus files)
  - Possible to inject more lethal payloads into the installers
  - Dell...switch...not sufficiently hardened
  - Fraudulent software (on ICX)...could change all...votes of any voter who selected this option
- **2019** — TX rejected DVS DS 5.5-A: including three issues making it not “safe from fraudulent or unauthorized manipulation”
What We Know

Threat and Vulnerability Indicators (2/2)

- **2019** – PA Report on DVS 5.5A: “system hardening measures...required additional modification for a secure implementation”
- **2020** – 35 voting systems found online THROUGH public internet
- **2020** – SolarWinds; 18k orgs (+DoD) >9 months to DISCOVER; fix? NEVER.
- **2020** – ~2 years: 100B credential attacks; 4B SQL injection/file attacks
- **2021** – Court approves FBI access/secure 100s of compromised MS Exch
- **2021** – Codecov Bash Upload script compromise DISCOVERED from Jan
- **2021** – Hidden RF modem chips discovered in MI ES&S Voting Machines
What We Don’t Know

The magnitude of compromise and exploitation, and by whom.
What we know is alarming.

What we don’t know is worse.

No system used in Colorado elections has EVER been adequately or persistently tested to determine vulnerability or compromise, nor monitored or defended.

No one who understands the threat would trust our system.
How can these vulnerabilities be exploited?

- **Voter fraud:** ANYBODY can be YOU or “<insert name>”
- **Election fraud:**
  - Enough <insert name> “Active,” but non-voting/non-existent “voters” to decide outcome
  - Insecure systems with voter, ballot, election status/data
  - PDF Ballots = anyone can print them – no fraudulent ballot detection mechanism
  - Mail-in/drop-box, + weak ID=voter verification is a façade
  - RLA opaque, tiny sample; ~checks machine error, not fraud
  - Everyone “knows” we have “The Gold Standard!” so the ballots, envelopes, machines, and systems are NEVER truly audited
When there’s smoke on the horizon, but no one on fire watch, who will notice the fire?

What We’ve Seen

There are significant and unexplained Colorado election indicators.
Indicators & Warnings – CO v. US Turnout

Voter turnout rates* among selected age groups in U.S. presidential elections from 1964 to 2016

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>60.7</td>
<td>67.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>62.2</td>
<td>71.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>58.6</td>
<td>70.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>60.2</td>
<td>72.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td>66.7</td>
<td>78.2</td>
<td>88</td>
<td>79</td>
<td>91</td>
</tr>
</tbody>
</table>

- CO turnout approximates compulsory-voting AUS
- Australia also has mobile teams at hospitals, nursing homes, and remote areas
What We’ve Seen

Indicators & Warnings – Statewide Turnout

CO Average Turnout: 78%

2020 a-historic older voter turnout surprised experienced Election Judges; because no healthcare facility Election Judges visited nursing homes to help older voters, as in past years.
In four counties (El Paso, Douglas, Weld, Mesa – 40% of all CO Active GOP voters), UAF voters cast ~same # of votes, at ~same time, as GOP votes? If that’s true, it’s unexplained.
Is someone tracking and matching GOP votes?
We did not observe the same consistent tight curve fitting in the top four major DEM counties. **WHY?**
WHY do UAF voters in DEM-dominant large counties behave differently than UAF in GOP-dominant large counties?
Why do UAF voters behave differently?

Depending on the dominant party in large CO counties?

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Candidate Votes</th>
<th>DEM Votes Recorded</th>
<th>REP Votes Recorded</th>
<th>UAF Votes Recorded</th>
<th>OTHER Votes Recorded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Donald J. Trump / Michael R. Pence</td>
<td>1,364,607</td>
<td>76,279</td>
<td>844,384</td>
<td>443,945</td>
<td>0</td>
</tr>
<tr>
<td>Joseph R. Biden / Kamala D. Harris</td>
<td>1,804,352</td>
<td>915,345</td>
<td>70,365</td>
<td>818,642</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>88,021</td>
<td>25,426</td>
<td>23,455</td>
<td>39,140</td>
<td>52,987</td>
</tr>
<tr>
<td>Grand Total</td>
<td>3,256,980</td>
<td>1,017,050</td>
<td>938,204</td>
<td>1,272,962</td>
<td>52,987</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>“Active” UAF Voters</th>
<th>Denver</th>
<th>ELP</th>
<th>Arapahoe</th>
<th>Jefferson</th>
<th>Adams</th>
<th>Larimer</th>
<th>Douglas</th>
<th>Weld</th>
<th>Boulder</th>
<th>Pueblo</th>
<th>Mesa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>184k</td>
<td>187k</td>
<td>168k</td>
<td>181k</td>
<td>123k</td>
<td>108k</td>
<td>104k</td>
<td>82k</td>
<td>95k</td>
<td>38k</td>
<td>42k</td>
</tr>
</tbody>
</table>

- 33% of U.S. voters are unaffiliated; 52% of those lean Dem; 48% of those lean GOP
- But not in CO, where UAF had to vote AT LEAST 62% DEM to negate GOP votes
- At some level of AMAZING turnout, especially in DEM-led counties, it will arouse suspicion
- But nobody was scrutinizing UAF “voters” in GOP-led counties
What We’ve Seen

Indicators & Warnings – Registration (El Paso)

Party Affiliation Breakdown Over Time

<table>
<thead>
<tr>
<th>Party</th>
<th>El Paso County</th>
<th>2016</th>
<th>2018</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEM</td>
<td>100,223</td>
<td>99,267</td>
<td>105,972</td>
<td></td>
</tr>
<tr>
<td>OTHER</td>
<td>9,984</td>
<td>10,820</td>
<td>12,386</td>
<td></td>
</tr>
<tr>
<td>REP</td>
<td>183,856</td>
<td>179,100</td>
<td>182,032</td>
<td></td>
</tr>
<tr>
<td>UAF</td>
<td>163,298</td>
<td>182,134</td>
<td>215,307</td>
<td></td>
</tr>
</tbody>
</table>

El Paso Voting Population by Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Voting Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>489,605</td>
</tr>
<tr>
<td>2015</td>
<td>496,422</td>
</tr>
<tr>
<td>2016</td>
<td>506,453</td>
</tr>
<tr>
<td>2018</td>
<td>618,090</td>
</tr>
<tr>
<td>2019</td>
<td>628,521</td>
</tr>
<tr>
<td>2020</td>
<td>540,412</td>
</tr>
<tr>
<td>2021</td>
<td>549,016</td>
</tr>
<tr>
<td>2022</td>
<td>557,734</td>
</tr>
</tbody>
</table>

Percent Change in Voting Population by Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Percent Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>1.37%</td>
</tr>
<tr>
<td>2015</td>
<td>2.02%</td>
</tr>
<tr>
<td>2017</td>
<td>2.30%</td>
</tr>
<tr>
<td>2019</td>
<td>2.25%</td>
</tr>
</tbody>
</table>

County level data retrieved from https://demography.dola.colorado.gov/population/data/county-data-lookup/
What We’ve Seen

Indicators & Warnings – Registration (Douglas)

Party Affiliation Breakdown Over Time

Douglas County

<table>
<thead>
<tr>
<th>Year</th>
<th>DEM</th>
<th>OTHER</th>
<th>REP</th>
<th>UAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>49,272</td>
<td>3,803</td>
<td>108,177</td>
<td>77,314</td>
</tr>
<tr>
<td>2018</td>
<td>49,838</td>
<td>3,867</td>
<td>106,346</td>
<td>91,582</td>
</tr>
<tr>
<td>2020</td>
<td>54,945</td>
<td>4,314</td>
<td>106,477</td>
<td>111,205</td>
</tr>
</tbody>
</table>

Douglas Voting Population by Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Voting Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>220,060</td>
</tr>
<tr>
<td>2016</td>
<td>228,454</td>
</tr>
<tr>
<td>2018</td>
<td>236,432</td>
</tr>
<tr>
<td>2020</td>
<td>251,995</td>
</tr>
<tr>
<td>2022</td>
<td>269,550</td>
</tr>
<tr>
<td>2024</td>
<td>276,688</td>
</tr>
</tbody>
</table>

Percent Change in Voting Population by Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Percent Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>3.81%</td>
</tr>
<tr>
<td>2015</td>
<td>3.49%</td>
</tr>
<tr>
<td>2017</td>
<td>3.05%</td>
</tr>
<tr>
<td>2019</td>
<td>3.42%</td>
</tr>
<tr>
<td>2021</td>
<td>3.31%</td>
</tr>
<tr>
<td>2023</td>
<td>3.53%</td>
</tr>
<tr>
<td>2025</td>
<td>2.65%</td>
</tr>
</tbody>
</table>

County level data retrieved from https://demography.data.colorado.gov/pollution/data/county-data-lookup/
## Indicators & Warnings – Registration Trends

**What We’ve Seen**

### Voter Registration Growth Over 4x Population Growth?

<table>
<thead>
<tr>
<th>Years</th>
<th>CO Population Growth</th>
<th>CO Voter Registration Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-2018</td>
<td>~154k</td>
<td>378k</td>
</tr>
<tr>
<td>2018-2020</td>
<td>~110k</td>
<td>471k</td>
</tr>
</tbody>
</table>
What Must Be Investigated

We MUST investigate to find or rule-out “fire.”
The Risk-Limiting Audit (RLA) is a Potemkin village:

*In theory,* “efficiently” predicts (SoS-chosen confidence-level), that machines correctly tabulated ballots. It cannot, even in theory, verify voters, ballots, or total counts. *In practice,* we cannot see the process of “random” selection, or exclusion, and “audit” samples are stunningly limited. We have traded integrity and transparency for efficiency.

A Potemkin village is any construction (literal or figurative) whose sole purpose is to provide an external façade to a country which is faring poorly, making people believe that the country is faring better.

Is there a fire? How can we find the truth?
Is there a fire? How can we find the truth?

Conduct a REAL audit to verify the integrity of our elections

A REAL audit requires independent / transparent:
• Voter Verification: Door-to-door, of state-reported voters
• Ballot/Envelope Verification: forensic exam/hand recount
• Image Verification: paper ballots match ballot images
• Tally Verification: images match cast vote records
• Reporting Verification: election night reports match tallies

Rawalpindi district, Pakistan completed door-to-door verification of 2.9M voters in 23 days in Dec ’15-Jan ’16

Andhra Pradesh state, India (49M) requires in-person voting, with voter ID, AFTER in-person voter verification.

“Voters Organized to Educate” went door-to-door (2019), to register ex-felons to vote, but verifying CO voting records are accurate is “intimidation/voter suppression?”
Fight to restore election integrity in Colorado!

Find & Spread the Truth: Demand Integrity!

• CITIZENS DESERVE to know the truth
• CITIZENS DESERVE leaders who SEEK and SPREAD truth
• Elected & Public officials MUST DEMAND the truth
• Finding the truth requires:
  • REAL AUDITS of voters, ballots, envelopes, systems & tallies
  • Ongoing, independent cybersecurity assessments (by Red Teams at NATION STATE-LEVEL ability) of:
    • SCORE & WebSCORE
    • All (Dominion, Clear Ballot, etc) voting systems
    • RLA Systems
    • BallotTrax
    • Reporting Systems (Clarity, Scytl, etc)
  • Vulnerability assessment for people, processes, and facilities/drop boxes
What Must Be Done

Restore integrity & trust – spread the truth and fix the system.
Restoring Integrity

“What the only way to be sure a network is clean is ‘to burn it down to the ground and rebuild it’...” Bruce Schneier

• **THIS** election architecture/system-of-systems cannot be “saved”
  • What was not secured from the beginning cannot EVER be secured
  • Audit and reform half-measures are placebos which will not restore integrity
• Under this system, will you know if you were duly elected, rather than “allowed” because you’re seen as tolerable, manipulable, or friendly?
• Without election integrity, and voter trust, who will vote for you?
• Citizens are fighting for election integrity – who will stand with us?

If not you, who? If not now, when?
What Must Be Done

Restoring Integrity

We need a system designed for integrity

• Accurate, county-controlled voter rolls (state gets read-only; has no access to alter)
  • 100% in-person voter verification on registration and, recurring, e.g. every two years
• Paper ballots
  • If mailed out to voters, then sequentially numbered or discretely identified
  • Mailed only AFTER active voter verification with return of voter postcard
• Government-issued photo-ID verified in-person to register, in-person to vote
• Vote in-person: all but UOCAVA and verified disability cast vote in-person, either
  • Mark the ballot at the VSPC, or
  • Hand over the previously-marked ballot (if mailed out to verified active registered voters)
• Scanning by machines that do not tabulate, cannot alter images, can only write to removable media (optical preferred, due USB vulnerabilities)
• Scanned images run through multiple, competing tabulators — any party can challenge; mismatched count mandates hand recount of paper ballots — wrong party(ies) pay the cost
• No counting until every ballot received (by deadline)
• No reporting until every received ballot scanned, counted, tabulated
Here’s the Deal

Be on the right side of history.
What it feels like to be us...

FOR GODS SAKE, TREVOR, ALWAYS YOU WITH THAT CONSPIRACY STUFF!

I’M TELLING YOU - THE MAN AND THE DOG ARE DEFINITELY WORKING TOGETHER...

How it feels trying to warn people about the true nature of government

“I see ‘Mr. Conspiracy Theory’ is at again”
The Idiot’s Idiom:

“The Gold Standard of Elections!”