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

How likely is it...cheating affected...outcome of...2020 Presidential election?

- "LIKELY:" 74% of Republicans, 30% of Democrats, 50% of UAF

What’s more important: Election Integrity or Voting Ease?
- "INTEGRITY:" 60% of voters (majorities in all racial groups)

CO Voter level of trust in our institutions?

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

CO Republican Voters feel?

"The government is rigged and run by liberal bureaucrats who stole the election."

THIS IS A CRISIS OF CONFIDENCE!
20 Yrs of “Efficiency” & “Accessibility”

...rather than Integrity


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

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.
It’s because the Emperor has No Clothes

CO Elections

Either:
- Our current system is immaculate, aka:
  “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.

What We Have

Thank you to the legislators who just stopped bills that undermine confidence in our elections and would have suppressed Coloradans’ right to vote.

The CO House State Affairs Committee protected your right to vote by killing 5 voter suppression bills today.
What We Have

CO Elections – The Narrative Begins...

SCORE: Statewide Voter Registration System
- SOS maintained and hosted software and hardware

Life of a Mail Ballot
- Ballot content: Voting instruction booklets, ballots, and official seal
- Ballot mailer handled: 20 days before the election, ballots to be returned to county clerk
- Voting: Ballots are mailed to eligible voters
- Ballot sorting: Election materials are returned to sorting
- Ballot pick up: Sorted ballots are mailed to state as requested
- Return ballott: Sorted ballots are mailed to state
- Signature verification: Ballots are rechecked after being mailed
- Envelope opening: Ballots are opened and reviewed for counting
- Counting & duplication: Ballots are counted and verified
- 8 days post election: Ballots are counted and verified
- Ballot results:_ballots are transmitted to the state by 8 PM

Election Management System (Dominion)
- County maintained software and hardware
- NCN internet connected county owned devices connected to central server

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

CO Risk-Limiting Audit

SCORE

DOMINION

CO Elections – A Systems Perspective

BALLOTTRAX

CLR CLEAR VOTE

TXT2Cure

What We Have

2,676 pieces of SoS-certified voting equipment

CO Risk-Limiting Audit
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 Packet 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?

Ballot Pick-Up
- “Bipartisan or "multipartisan?" e.g. “Democrat & "Social Democrat"
- “Secure?"

Return Ballot
- “Secure?”
- Video ever reviewed?
- What security with the U.S. Postal Service?
CO Elections – Reasonable Questions

What We Have

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?

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

Counting & Duplication
- Duplication BEFORE counting?
- Is “Adjudication” a software application, a procedure, or a function?

Signature Verification
Ballots with signatures that match voter record proceed. If not verified voter is notified they must resolve discrepancy for ballots to proceed.

Envelope Opening
Ballots are removed from envelope maintaining secrecy and prepared for counting.

Counting & Duplication
During counting ballots damaged or with unclear marks are reviewed by bipartisan teams and adjudicated.

Audit / Certification
- Do election judges have ANY idea what happens inside computers?
- Does the public EVER get access to examine the ballots stored for 25 mos? If not, why keep them?
CO Elections – Reasonable Questions

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

What We Have
What We Have

CO Elections – Registration Systems

• SCORE – Statewide Colorado Registration & Election system – 2008
  • Registered voter database, signature repository; ballot tracking; epollbook*
  • HP/SaBER Corp base code (Electus)

• SABER “security testing” wasn’t; it was functional testing
  • 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
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)
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
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”
CO Elections – Process Vulnerabilities

What We Know

• 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 is 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
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&amp;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
## Systems Vulnerabilities (3/10)

### 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)

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

### CO Elections – Systems Vulnerabilities (7/10)

<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>Web Server</td>
<td>H</td>
<td>Proprietary</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></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>

31
## CO Elections – Systems Vulnerabilities (9/10)

**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 (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>
What We Know

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
• 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 Don’t Know

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
What We’ve Seen

There are significant and unexplained Colorado election indicators.

When there’s smoke on the horizon, but no one on fire watch, who will notice the fire?
Indicators & Warnings – CO v. US Turnout

What We’ve Seen

CO turnout %, VEP v. U.S.

- 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

- 2020 a-historic older voter turnout
- Surprised experienced Election Judges, because no health facilities Election Judges visiting 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.
Indicators & Warnings – UAF v. GOP Voters

What We’ve Seen

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>

What We’ve Seen

- 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
El Paso 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>100,223</td>
<td>9,084</td>
<td>183,858</td>
<td>163,298</td>
</tr>
<tr>
<td>2018</td>
<td>59,267</td>
<td>10,828</td>
<td>179,100</td>
<td>182,134</td>
</tr>
<tr>
<td>2020</td>
<td>105,972</td>
<td>12,386</td>
<td>182,032</td>
<td>215,307</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>489,695</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>2020</td>
<td>549,016</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>2014</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/pollingdata/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>77,814</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>243,650</td>
</tr>
<tr>
<td>2020</td>
<td>269,550</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>2.65%</td>
</tr>
</tbody>
</table>

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

<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>

Voter Registration Growth Over 4x Population Growth?
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?
What Must Be Investigated

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 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)
➔ 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

“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?
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 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)
  • 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.
The Idiot’s Idiom:

“THE GOLD STANDARD OF ELECTIONS!”