Enemy Inside the Wire

COL SHAWN SMITH (RET)

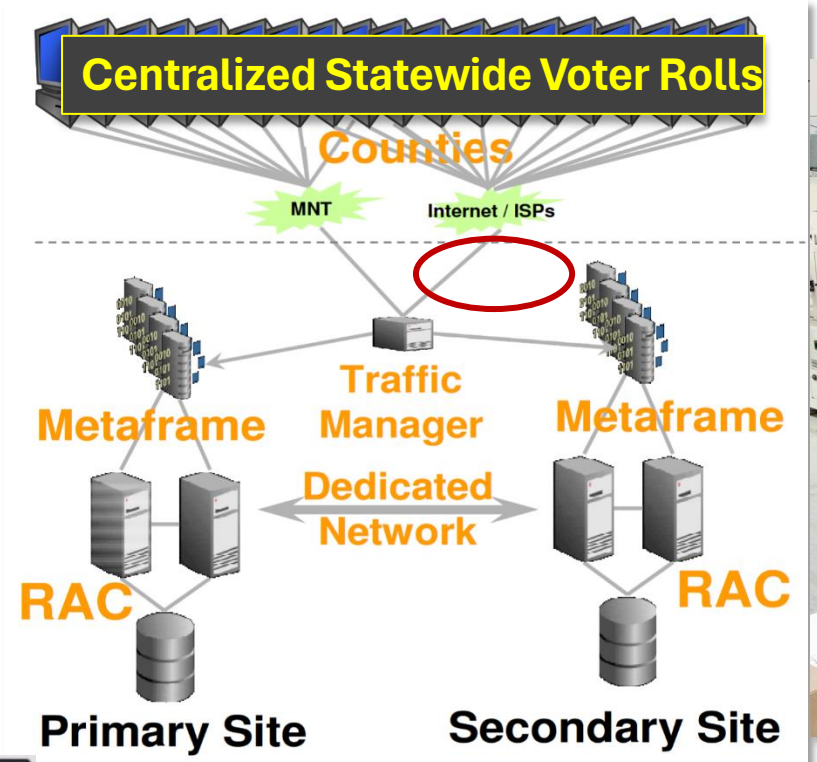
LINDELLPLAN.COM

Restoring National Confidence Summit

LINDELL TEAM

The Election System We Have

Centralized Statewide Voter Rolls



Industrial Vendor Ballot Printing

Vendor Access to Central Rolls

The Runbeck team has successfully implemented the API for the Agilis to integrate with SCORE for signature capture and verification. This interface allows the Agilis software to download and upload voter and signature files

USPS Delivery/Return

Vendor Access to Central Rolls/USPS

6.2.5 Section V: Source Code Access and E

Ballot Tracking is not covered under the current EAC guidelines, for this reason and the fact that our software works in a SaaS (Software as a Service) environment, i3logix will not disclose the source code of i3ballot or submit such to escrow.

Vendor Return/Scanning/SigVer

All before the first vote is counted.

The Election System We Have

ES&S

Dominion

Hart-InterCivic

Unisyn

Clear Ballot Group

It's ALL Machines.

Systems Made Entirely in U.S., of U.S. Parts

None.

The Threat

“The exploitation of key supply chains by foreign adversaries—especially when executed in concert with cyber intrusions and insider threat activities—represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure…

SolarWinds was a Supply-Chain Attack.

12

The Threat

…Foreign adversaries are attempting to access our nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance—by inserting malware into important information technology networks and communications systems…

Centrifuge Sabotage at Natanz was a Supply-Chain Attack.

The Threat

…The increasing reliance on foreign-owned or controlled hardware, software, or services as well as the proliferation of networking technologies, including those associated with the Internet of Things, creates vulnerabilities in our nation's supply chains…

2023 S-C Attacks: Airbus, Norton, Microsoft, Colonial Pipeline…

The Threat

…By exploiting these vulnerabilities, foreign adversaries could compromise the integrity, trustworthiness, and authenticity of products and services that underpin government and American industry, or even subvert and disrupt critical networks and systems, operations, products, and weapons platforms in a time of crisis."

National Counterintelligence and Security Center, "Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains" - 25 September 2020

SolarWinds was TWO Attacks

The Threat

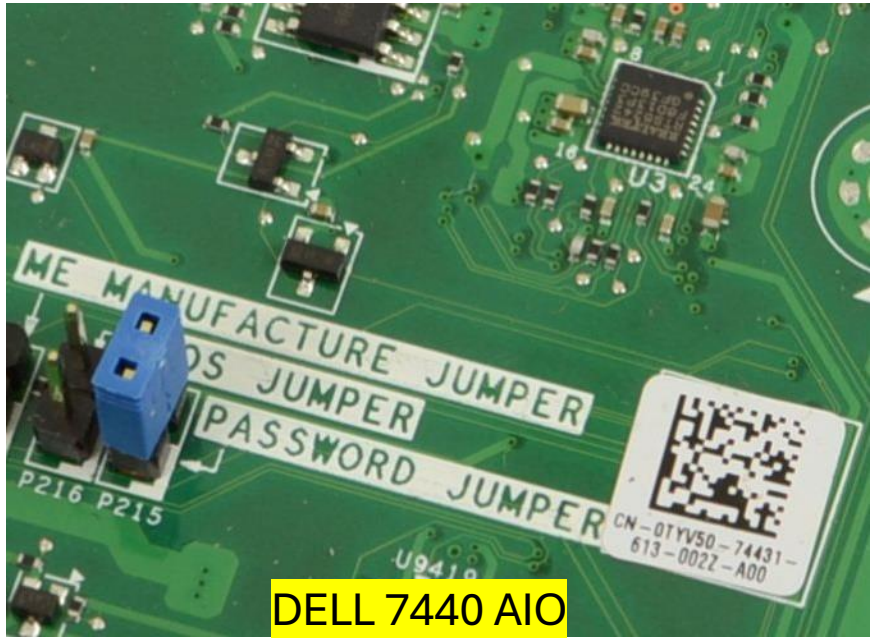
“Without effective security processes and practices throughout the life cycle of a system, intentional and unintentional vulnerabilities can be placed into systems. The systems may then be exploited by attackers who insert malicious content, capture data or take other advantages, resulting in untrustworthy products or services, unanticipated failure rates, or compromise of federal missions and information”

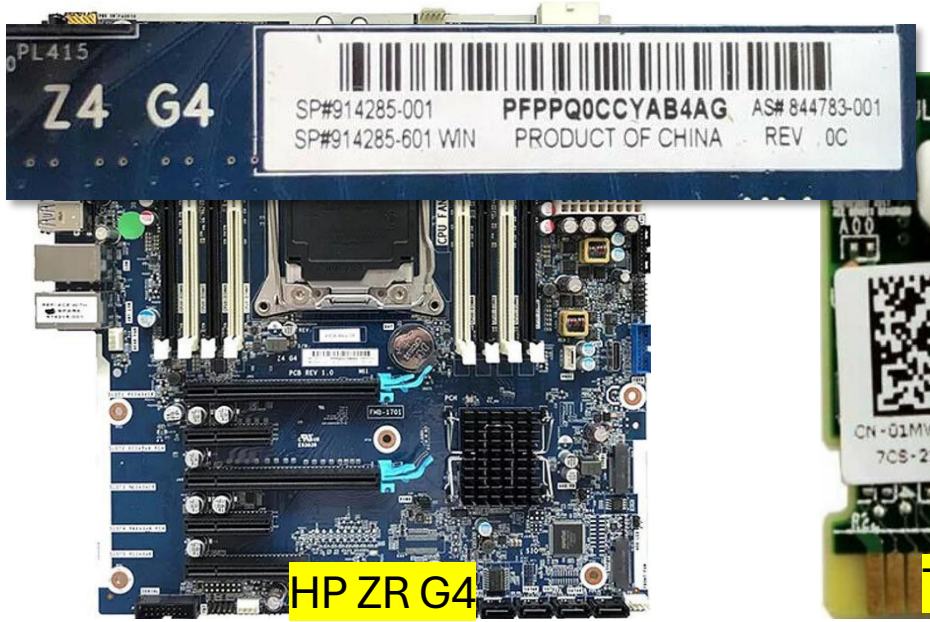
- NIST Information Technology Bulletin, June 2015

https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2015-06.pdf

29 of 37 Publicly Acknowledged APTs are PRC.

The Threat – Enemy Inside The Wire

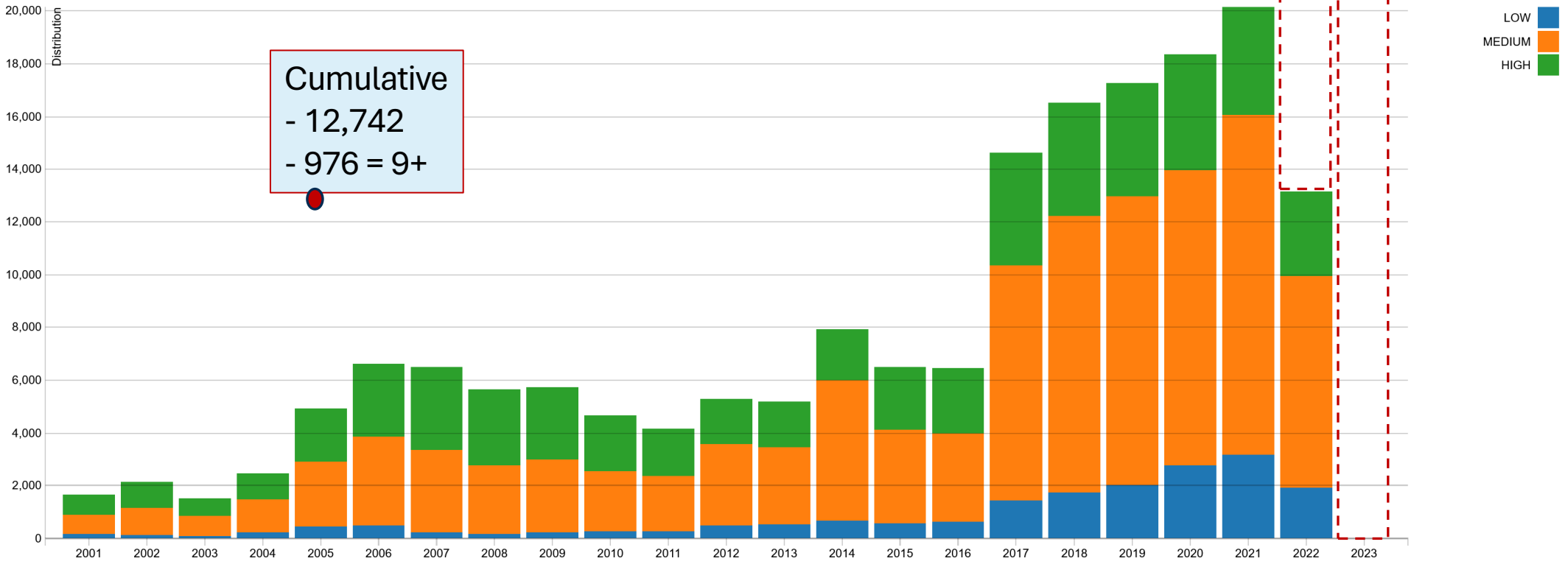




The Threat – Known Vulnerabilities

CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page .



The Defense

Election systems = “critical infrastructure”

Federal standards/testing/certification

Configuration control

State Testing: Acceptance/Logic & Accuracy

Audits

“Election Experts”

19

The Defense – Critical Infrastructure

DoD on Critical Infrastructure:

- 2012: Requires trusted suppliers, supply-chain security, configuration IAW Security Technical Implementation Guides (STIG)
- 2015: Advanced Persistent Threat (APT) breach Joint Staff email
- 2020: DoD, et al, breached by SolarWinds APT compromise – undetected for 10+ months

DHS, re: Election Systems:

- No standards, testing, enforcement for rolls, pollbooks, audits
- Voting system standards, testing, certification left to EAC
- CISA is responsible for election cybersecurity – also breached by SolarWinds compromise – undetected for 10+ months

The Defense – Standards

FEC 2002 Voting System Standards (VSS); EAC 2005, 2015, 2021 Voluntary Voting System Guidelines (VVSG)

U.S. voting systems EAC-certified to

- **VVSG 1.1 (2015): 0**
- **VVSG 2.0 (2021): 0**

No U.S. voting system is certified to a standard newer than 18 years old

No standard before 2021 even mentions supply chain security; 2021 requires a plan – no enforcement, no metric

The Defense – Voting System Test/Certification

- **Voting System Testing Lab (VSTL) accreditations expired – EAC, SoSs lied, made illegal certifications**
- **EAC/election officials repeatedly fail to detect/prevent corruption, uncertified components & systems**
- **Director of 1 of 2 VSTLs:"…actually claims no specialized knowledge or background in cybersecurity engineering…"**

Williamson, DeKalb, Maricopa, Mesa, Northhampton…

22

The Defense – Configuration Control

- Engineering Change Orders (ECO) – 1) Vendor Notification, 2) VSTL assessment, 3) EAC Decision
- "De Minimis" = no independent testing of ECO
- 171 ECOs in EAC database
  - 35 in the last 12 months, include entirely new computers, central processors, BIOS, firmware, operating systems – all "de minimis"
  - E.g. Clear Ballot added Lenovo ThinkPad E14 w/COTS software – "de minimis" – DoD warning? 2016
- No monitoring, no enforcement

The Defense – User Testing: Acceptance/L&A

- VSTLs test an *example* of a voting system *version*
- *NOBODY* tests 99.999% of U.S. voting systems. *Ever.*
- State acceptance testing is purely functional, if at all
- Logic & Accuracy (L&A) testing is an anachronism from the days of mechanical voting systems
  - Public officials do not have the expertise, authority, or time
  - If they did, *still* couldn't adequately test complex systems
  - L&A is a puppet show – it does nothing, it proves nothing
  - Sold as "verifying security and accuracy" – it cannot

The Defense – Audits

- "Auditable" means *nothing* – an unworn seatbelt
- Paper ballots are no safeguard unless you audit them
- "Trust us!" institutions pushing "risk-limiting audits"
  - Originator (Stark) disavows how they are being used
  - Cannot prove accurate election result
  - Cannot detect fraud
- Williamson & DeKalb, etc., prove hand-count of paper ballots is the ONLY way to reliably detect machine error & fraud

The Defense – With Experts Like These…

“The November 3rd election was the most secure in American history.”

Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees – 12 November 2020

CISA Assistant Director Bob Kolasky

U.S. EAC Chair Benjamin Hovland

NASS President President Maggie Toulouse Oliver

NASED President Lori Augino

Escambia, FL Supervisor of Elections David Stafford

Chair Brian Hancock (Unisyn Voting Solutions)

Vice Chair Sam Derheimer (Hart InterCivic)

Chris Wlaschin (Election Systems & Software)

Ericka Haas (Electronic Registration Info. Center)

Maria Bianchi (Democracy Works)

The Election System We Have

Centralized, vulnerable, dirty voter rolls

Vulnerable mail-in ballots & lax ID

Vulnerable black-box vote counting

Vulnerable vendor-controlled reporting

Vulnerable black-box election audits

No way to verify HOW your vote counted

*Vulnerable to **fake voters, fake ballots, fake counts***

The Warnings

Collier brothers, Votescam, 1992: “Computers in voting machines are effectively immune from checking and rechecking. If they are fixed, you cannot know it, and you cannot be at all sure of an honest tally.”

Bev Harris, Black Box Voting, 2004: “With computerized voting, the certified and sworn officials step aside and let technicians, and sometimes the county computer guy, tell us the election results.”

Sheila Parks, While We Still Have Time, 2012: “Elections using electronic voting machines are often rigged by deliberately not counting the votes as cast.”

Gould report, Mesa County, September 2021: “(CRS) 1-5-601.5 requires…compliance with…2002 Voting System Standards…this forensic examination found that a substantially large number of these requirements have not been met.”

Halderman Declaration, 1:17-CV-2989-AT, Curling v. Raffensberger:“My July 1, 2021, expert report describes…flaws that would allow attackers to install malicious software on the ICX,…with temporary physical access…or remotely from (EMS)…Nor do these problems affect (GA) alone…It will be used for accessible voting in…Colorado”

The Truth

Foreign-built systems/components have not been, are not now, and will never be secure.

Complex systems will never be secure or securable.

Anyone telling you these systems are secure either has no idea what they're saying or they're lying.

The "safeguards" aren't safe. They're not even real.

U.S. built computer-based voting systems are not the answer – citizens still cannot verify the truth for themselves.

The Election System We Need

Component	Prevents Fake Voters	Prevents Fake Ballots	Prevents Fake Counts
Start over: Locally-controlled, clean voter rolls	☑		
In-person, election DAY voting w/gov. photo ID	☑	☑	
Precinct hand-count of numbered ballots under live-streamed, archived HD video		☑	☑
Precincts certify and report vote count to precinct VOTERS, *then Report certified count to counties*			☑
Counties tally precinct counts ON VIDEO, report certified tally to voters/states			☑
States tally counties' tallies, report/certify to voters			☑