Vol 4. - "The Global Architecture of Election Control: How Federal and State Actors, Private Vendors, and International Influence Undermine Transparency and National Sovereignty"

Unveiling the Architecture of Election Security Vulnerabilities

The integrity of American elections has long been heralded as the cornerstone of democracy, yet in recent years, revelations about systemic weaknesses have exposed a troubling dichotomy: while federal and state agencies espouse commitments to security and transparency, their actions reveal deliberate obfuscation, negligence, and, at times, willful complicity in undermining the nation's electoral processes. Volume 4 of this investigation delves into the deceptive practices, unaccountable governance, and federal overreach that have reshaped election systems into opaque and untrustworthy structures, endangering both national security and public confidence.

This volume builds on the foundation laid in previous volumes, meticulously unraveling how federal advisory agencies such as the **Cybersecurity and Infrastructure Security Agency (CISA)** and the **Election Assistance Commission (EAC)** have exceeded their advisory roles to dictate state election policies. Under the guise of "best practices," these agencies sidestep mandatory federal cybersecurity standards like the **NIST Cybersecurity Framework (CSF)** while proliferating narratives that suppress public scrutiny and accountability.

Central to this volume is the exploration of how state officials, relying on guidance from federal entities, have institutionalized practices that prioritize security theater over substantive protections. By leveraging legislative and administrative tools, they have systematically restricted access to critical election records, diluted transparency, and obscured vulnerabilities in voting systems. These actions contravene **Executive Order 13800**, which mandates robust cybersecurity measures for critical infrastructure, including elections, making noncompliance a direct threat to national security.

The report also highlights the complicity of private vendors, whose proprietary software and reliance on third-party dependencies create exploitable vulnerabilities. Despite repeated evidence of systemic risks—such as the infiltration vectors exposed through the ***SolarWinds Orion breach*** and the pervasive risks of outdated software—there remains no meaningful accountability. Vendors operate under a veil of secrecy, shielded by misapplications of laws like the ***Trade Secrets Act***, perpetuating an environment where transparency is viewed as a threat rather than a safeguard.

As this investigation demonstrates, the dysfunction within the election security framework extends beyond negligence to deliberate actions that prioritize control over compliance. From the refusal to allow independent audits to the suppression of cast vote records, and from the promotion of risk-limiting audits that compromise voter anonymity to the adoption of cloud-based systems vulnerable to exploitation, the actions of these entities represent a betrayal of their constitutional obligations to protect the republic.

Building on the foundational principles of federal law and the constitutional mandate to secure elections as critical infrastructure, this report scrutinizes the tangible ways in which federal advisory agencies, state officials, and private entities have collaborated to sidestep these responsibilities. What follows is an in-depth examination of how this coordinated framework—designed under the pretense of enhancing election security—has systematically dismantled the very safeguards it claims to uphold.

Under the guise of enhancing election security, federal agencies like **CISA** and the **EAC**, in coordination with state election officials, have implemented a framework that centralizes control over election processes, restricts transparency, and violates both federal mandates and constitutional protections. Documentation from internal communications, regulatory amendments, and legislative actions exposes the depth of this coordination, revealing how these measures, presented as safeguards, systematically obstruct independent oversight. These actions, far from bolstering public trust, undermine voter privacy and defy established laws designed to protect critical infrastructure and uphold democratic processes.

The catalyst for this centralized framework can be traced back to the 2017 decision by the Obama administration to designate elections as critical infrastructure under the **Department of Homeland Security (DHS)**. This designation, while ostensibly aimed at protecting elections from foreign interference, gave federal agencies like **CISA**

significant influence over state-administered elections. **CISA's** involvement has grown to include prescriptive guidance on election security practices, including chain-of-custody protocols, risk-limiting audits (RLAs), and public communication strategies.

In January 2022, **CISA** consultants Noah Praetz and Jennifer Morrell delivered a presentation to state election officials promoting the ***"Track, Test, Tell" framework***. This presentation emphasized strict adherence to chain-of-custody protocols and RLAs, portraying these measures as critical to ensuring election integrity. However, these protocols introduce significant concerns. The chain-of-custody requirements rely on advanced mail-sorting equipment, such as **Runbeck** and **BlueCrest** systems, which imprint both envelopes and ballots with unique sequential markers. These imprints, combined with cloud storage solutions like **Microsoft Azure**, create a filing system that ties voter signatures to corresponding ballots, fundamentally compromising voter anonymity. While RLAs are marketed as a security enhancement, their reliance on this infrastructure effectively creates a mechanism for tracking individual votes—a reality election officials have gone to great lengths to conceal.

Washington State provides a case study in how this system has been implemented and institutionalized. Documentation from the **Office of the Secretary of State (OSOS)**, particularly under **Stuart Holmes**, shows how administrative actions and legislative measures have been used to restrict transparency and block independent oversight. Holmes issued a **clearinghouse notice** tying **Washington's** election systems to certification standards of the **EAC,** an advisory body initially tasked with distributing grants and providing best practices under the **Help America Vote Act (HAVA)**. Over time, the **EAC** expanded its role to include certifying election systems—a shift that has drawn criticism for its lack of enforcement authority and alignment with **CISA** and **DHS**. This alignment reflects a broader trend of federal advisory agencies exceeding their mandates to exert control over state election processes.

Holmes' notice also introduced amendments to **WAC 434-335-260**, which explicitly prohibited third-party access to voting systems for independent testing or compliance verification. These restrictions directly contravene **Executive Order 13800**, which mandates adherence to **NIST cybersecurity frameworks** for critical infrastructure. **EO 13800** requires independent assessments to verify compliance, yet the **WAC** amendments insulated **Washington's** election systems from such scrutiny. This strategy was later codified through the passage of **SB5459** in 2023, which removed **cast vote**

records (**CVRs**) and election security information from public records, further solidifying the lack of transparency.

The refusal to release **CVRs** predates **SB5459**, demonstrating a deliberate, coordinated effort to block public access to these critical records. **CVRs**, which are digital summaries of ballots, are integral to independent audits and election verification. Despite this, every county in **Washington**, as well as the **OSOS**, has repeatedly denied requests for **CVRs**, citing legal pretexts that do not withstand scrutiny. For example, the conflation of ballot secrecy with the transparency of aggregated voting data has been used to justify these denials. However, the true reason for withholding **CVRs** lies in the sequential markers imprinted on ballots and envelopes, which enable the cross-referencing of voter signatures with their votes. This capability is essential for RLAs, where election staff must locate specific ballots within batches based on their digital images, but it also exposes a systemic vulnerability to privacy violations.

CISA's dual role in promoting RLAs while advising states to restrict access to election records under the pretense of "security concerns" reveals a troubling inconsistency. The very protocols designed to enhance transparency and security facilitate the creation of a system that undermines voter privacy. This contradiction is exacerbated by legislative and administrative measures that codify opacity into law, ensuring that these vulnerabilities remain hidden from public scrutiny.

From a constitutional perspective, these actions raise serious legal questions. ***The Supremacy Clause (Article VI of the U.S. Constitution)*** establishes that federal law takes precedence over conflicting state regulations. **Washington's** refusal to allow third-party audits and its exclusion of CVRs from public access conflict directly with **EO 13800** and the **NIST cybersecurity frameworks**. Furthermore, ***Marbury v. Madison (1803)*** affirms that laws repugnant to the Constitution are void and unenforceable. By obstructing independent oversight and codifying secrecy, **Washington's** legislative and administrative actions are unconstitutional.

"The general misconception is that any statute passed by legislators bearing the appearance of law constitutes the law of the land. The U.S. Constitution is the supreme law of the land, and any statute, to be valid, must be in agreement. It is impossible for both the Constitution and a law violating it to be valid; one must

prevail. This is succinctly stated as follows:The General rule is that an unconstitutional statute, though having the form and name of law is in reality no law, but is wholly void and ineffective for any purpose; since unconstitutionality dates from the time of its enactment and not merely from the date of the decision so branding it. An unconstitutional law, in legal contemplation, is as inoperative as if it had never been passed. Such a statute leaves the question that it purports to settle just as it would be had the statute not been enacted. Since an unconstitutional law is void, the general principles follow that it imposes no duties, confers no rights, creates no office, bestows no power or authority on anyone, affords no protection, and justifies no acts performed under it. A void act cannot be legally consistent with a valid one. An unconstitutional law cannot operate to supersede any existing valid law. Indeed, insofar as a statute runs counter to the fundamental law of the land, it is superseded thereby. No one is bound to obey an unconstitutional law and no courts are bound to enforce it."
(16 American Jurisprudence 2d, Sec 177 late 2d, Sec 256.)

"Generally statute leaves the question that it purports to settle just as it would be had the statute not been enacted. Since an unconstitutional law is void, the general principles follow that it Pg 126imposes no duties, confers no rights, creates no office, bestows no power or authority on anyone, affords no protection, and justifies no acts performed under it. A contract which rests on

an unconstitutional statute creates no obligation to be impaired by subsequent legislation."

(American Jurisprudence 2nd 1964 vol. 16 CONSTITUTIONAL LAW § 177.)

"No one is bound to obey an unconstitutional law and no courts are bound to enforce it. Indeed, insofar as a statute runs counter to the fundamental law of the land, it is superseded thereby. It is said that all persons are presumed to know the law, meaning that ignorance of the law excuses no one; if any person acts under an unconstitutional statute, he does so at his peril and must take the consequences."

(Pg. 403 – 405 16 American Jurisprudence 2d., Const. Law Sec. 70.)

The broader implications of these practices extend beyond **Washington State.** The alignment of federal advisory agencies with state election offices reflects a national trend toward centralizing control over election systems. This centralization undermines the independence and transparency of state-administered elections, eroding public trust in the democratic process. The exclusion of third-party audits, the suppression of **CVRs**, and the reliance on systems that compromise voter privacy represent a clear and present danger to election integrity.

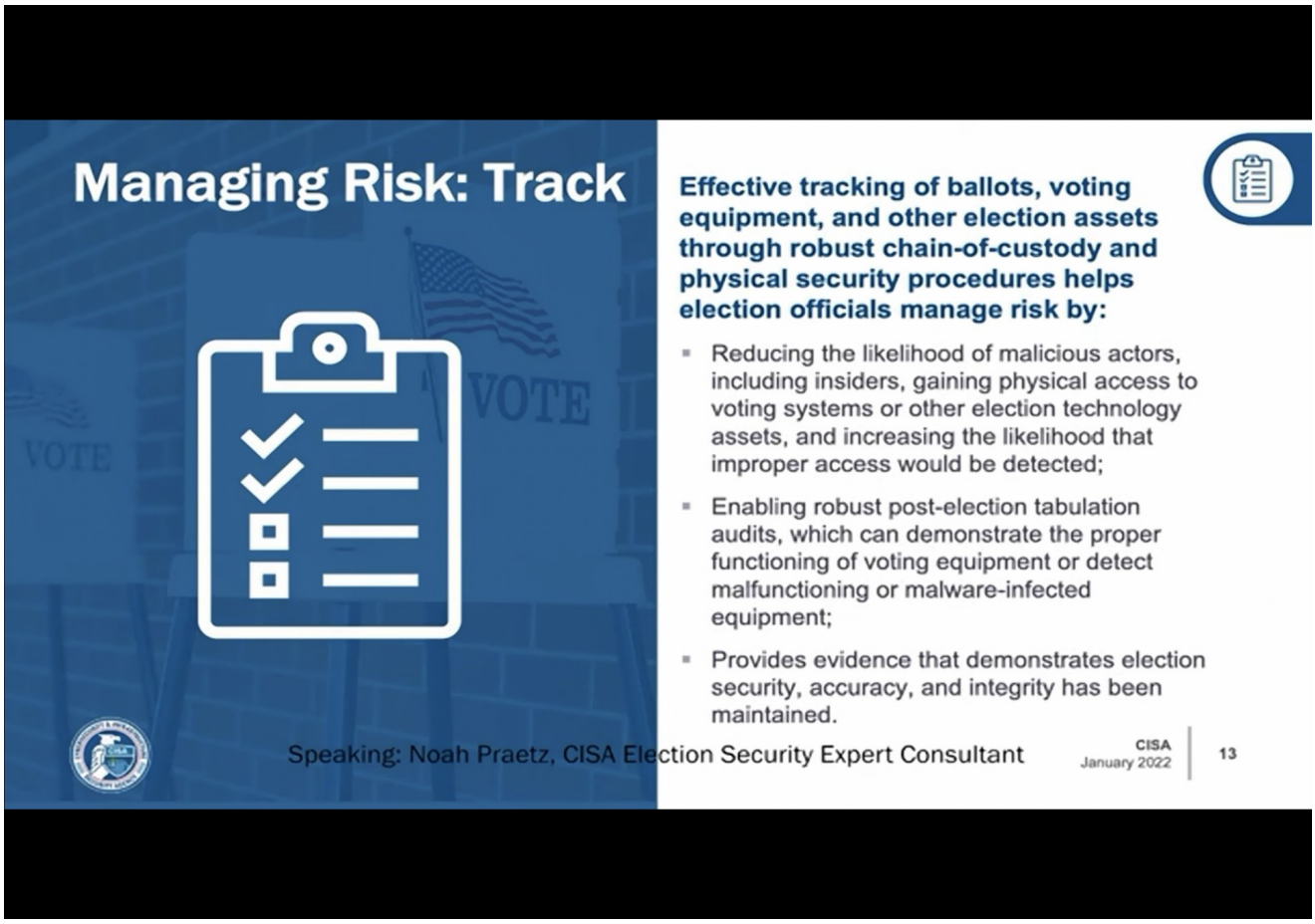
These violations are not merely procedural oversights; they represent a systematic and coordinated effort to obstruct transparency, suppress public access, and sidestep federal cybersecurity mandates. Executive Order 13800 and the NIST Cybersecurity Framework (CSF) clearly define the obligations of state election systems as critical infrastructure, requiring independent assessments and adherence to robust security standards. Yet Washington's state officials—including legislators, the Attorney General (AG), the Secretary of State (SOS), auditors, and even unelected roles like the elections director—have failed to uphold these requirements. While these officials hold positions defined by law as fiduciaries of the public trust, their actions and omissions reveal a pattern of willful negligence and, in some cases, direct violations of state and federal laws.

The **Attorney General**, **Bob Ferguson,** plays a particularly troubling role in this failure. Under **RCW 42.56.530**, when any person is denied records by a state agency, the **AG** is required to issue a written opinion on the matter upon request. Yet, when the **OSOS** denied access to cast vote records, Ferguson refused to provide the mandated written opinion, depriving the public of even the procedural remedy guaranteed under Washington law. This refusal is itself a violation of **RCW 42.56.530**, compounding the lack of transparency already entrenched in Washington's election system.

Ferguson's influence extends further through his approval of state contract matrices that sidestep **EO 13800**. These matrices allow vendors and contractors responsible for election infrastructure to self-assess their compliance with state security standards, bypassing the **NIST CSF** mandated for critical infrastructure by federal law. This deliberate workaround not only undermines the integrity of election security but also flagrantly disregards federal mandates that prioritize independent verification and third-party audits.

State officers, including the **AG**, **SOS**, **legislators**, and **auditors**, are bound by the **Constitution** and federal law to ensure lawful governance. As clarified in ***Hafer v. Melo (502 U.S. 21, 1991),*** *"State officers may be held personally liable for damages based upon actions taken in their official capacities."* This accountability applies equally to unelected roles like the elections director, whose lack of an oath or bond underscores the structural failures in the system they oversee. Furthermore, ***Marbury v. Madison*** and foundational principles in ***American Jurisprudence*** affirm that any law or action repugnant to the Constitution is void and imposes no obligation. These officials, by actively undermining federal mandates, obstructing transparency, and insulating election systems from scrutiny, expose themselves to personal and legal liability for their actions.

To disregard Constitutional law, and to violate the same, creates a sure liability upon the one involved: "State officers may be held personally liable for damages based upon actions taken in their official capacities."
(Hafer v. Melo, 502 U.S. 21. 1991).


Managing Risk: Track
Effective tracking of ballots, voting equipment, and other election assets through robust chain-of-custody and physical security procedures helps election officials manage risk by:
Reducing the likelihood of malicious actors, including insiders, gaining physical access to voting systems or other election technology assets, and increasing the likelihood that improper access would be detected;
Enabling robust post-election tabulation audits, which can demonstrate the proper functioning of voting equipment or detect malfunctioning or malware-infected equipment;
Provides evidence that demonstrates election security, accuracy, and integrity has been maintained.
Speaking: Noah Praetz, CISA Election Security Expert Consultant
CISA
January 2022
13

How Can Election Officials Help? The Three Ts

Track

Document your cybersecurity, physical security, and operational security processes and procedures to ensure that safeguards are enacted and implemented.

Test

Verify and audit your processes and procedures, the work of your staff, and the functioning of election infrastructure.

Tell

Provide fact-based evidence of why your voters should trust elections and get ahead of likely stories by pre-bunking false narratives before they catch hold, and then quickly rebutting them if they do start to spread.

Track: Standard Operating Procedures

Written Standard Operating Procedures (SOPs) can:

- Limit risks to the operation of election infrastructure
- Limit ad hoc decision making
- Increase quality and consistency of work across staff
- Increase productivity, efficiency and measurement opportunities
- Speed remediation time when following incident response plans

SOPs for each procedure or operation should:

- Provide sequential steps for each process and be extensively detailed
- Include visual depictions along with examples for completing forms
- Include checklists and logs used for verification

Track: Control Forms

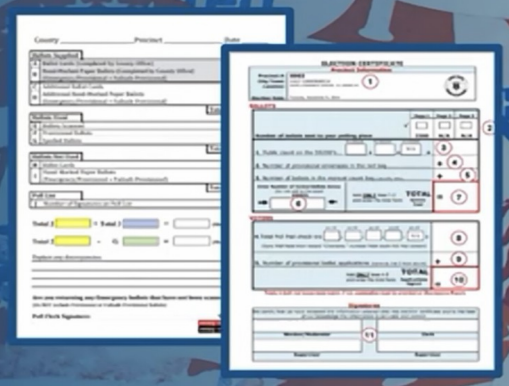
Control forms capture data with precision at critical points in time and provide evidence for audits or incident analysis

Control forms include things like:

- Chain of custody documentation
- Secure location entry and exit logs
- Ballot duplication logs
- ENR uploads

Forms not filled out completely or neatly can lead to problems:

- Ensure good form design
- Use multi-person verification to ensure accuracy and completeness
- Pre-fill as much information as possible or use automation software



Track: Assets

Movements of assets, people, materials, and data should be tracked to manage access controls risks.

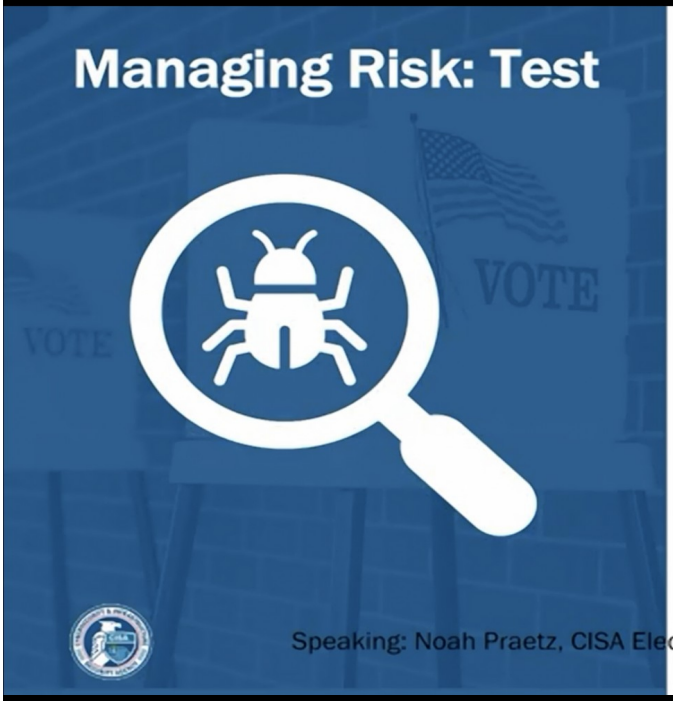
Automating the tracking process can make it easier to capture what is happening and when.

What aren't you currently tracking that you can/should?

For Example:

- Election equipment (voting equipment, mail ballot sorters, signature verification, asset management, etc.) as it moves from resting storage state to testing, to production, to post-election testing, and back to storage
- Mail ballots being moved from receipt to verification to opening to scanning, to auditing, and to permanent storage

Managing Risk: Test



Robust testing and auditing of voting equipment and other election assets and processes help election officials manage risk by:

- Demonstrating the proper functioning of voting equipment and other election assets or detecting malfunctioning or malware-infected equipment
- Identifying strengths and weaknesses in the election office's cybersecurity and physical security risk posture
- Ensuring that election workers are operating in the secure manner proscribed in your standard operating procedures (SOPs)

Speaking: Noah Praetz, CISA Election Security Expert Consultant

Test: Election Audits

Post-Election Tabulation Audits

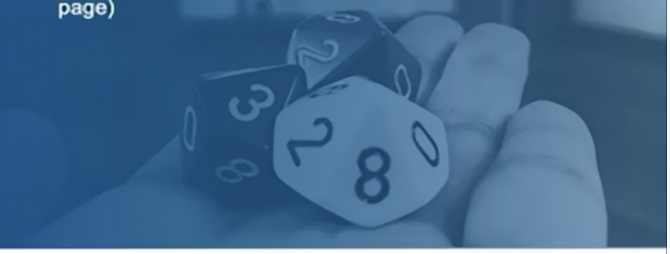
- A post-election tabulation audit is the act of reviewing a sample of voted ballots against the results produced by the voting system to ensure accuracy.
- A risk-limiting audit (RLA) is a type of post-election tabulation audit that examines a random sample from all voted ballots to provide a statistical level of confidence that the outcome of the election is correct.

Any audit, not just tabulation audits, should provide election officials with a way to:

- Detect voting system errors; human error, misconfiguration or manipulation
- Provide accountability to voters
- Deter fraudulent activity
- Assure ballots issued, counted, and reported accurately
- Provide feedback for process improvement

Systems you should audit include:

- Voting Systems
- Voter Registration Systems
- Signature Verification Systems (ASR & manual)
- Mail Ballot Sorters (including ASR/ASV function)
- ePollbooks
- Website tools (voter lookup, polling location finders, ENR page)



Speaking: Jennifer Morrell, CISA Election Security Expert Consultant

Test: Compliance Audits

Informal compliance audits ensure standard operating procedures (SOPs) work. This can be used to test:

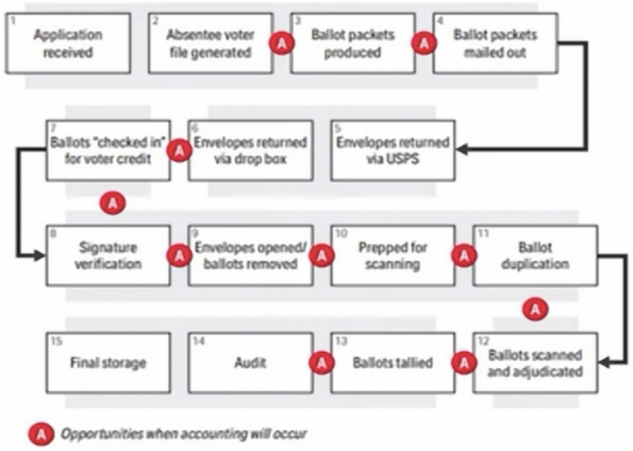
- Workflow
- Necessary equipment and supplies
- Form design
- Effectiveness of training

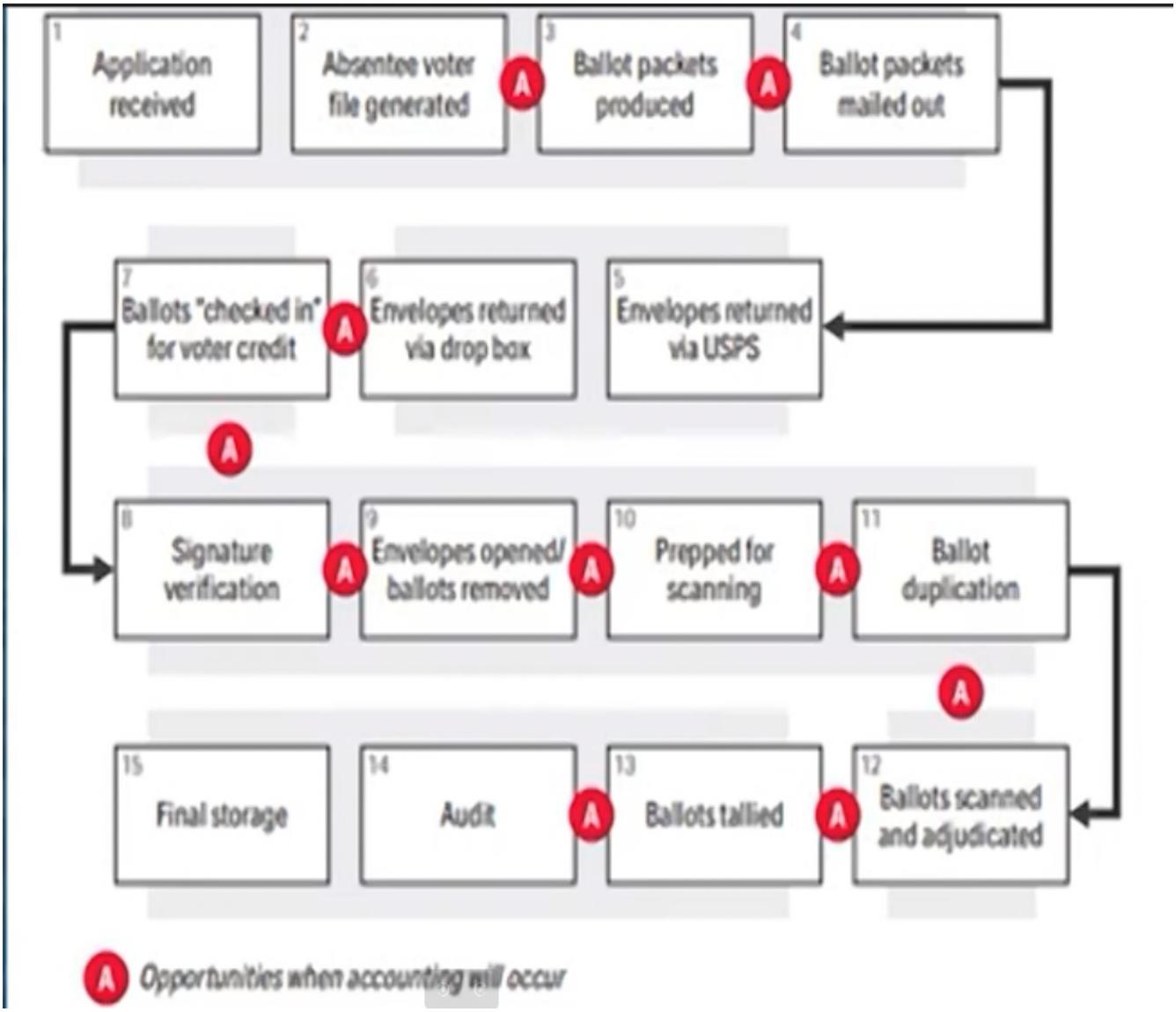
Formal compliance audits ensure SOPs are being followed. These might be conducted by:

- Election authority or supervisor
- External office

Test: Other Audits

- Systematic audits of the voter registration database
- GIS audits for correct voter and district assignments
- Security audits
- Ballot reconciliation/chain of custody audits
- Ballot layout and design audits
- Resource allocation audits to ensuring enough equipment, supplies, and people have been allocated to meet demand




1
Application received
2
Absentee voter file generated
A
3
Ballot packets produced
A
4
Ballot packets mailed out
7
Ballots "checked in" for voter credit
A
6
Envelopes returned via drop box
5
Envelopes returned via USPS
A
8
Signature verification
A
9
Envelopes opened/ ballots removed
A
10
Prepped for scanning
A
11
Ballot duplication
A
15
Final storage
14
Audit
A
13
Ballots tallied
A
12
Ballots scanned and adjudicated
A Opportunities when accounting will occur



Proactive and responsive communications and transparency measures help election officials manage risk by:

- Bolstering public resilience against MDM narratives and claims;
- Educating voters and the broader public about cybersecurity and physical risks to election infrastructure and the controls put in place to manage such risks; and
- Enabling meaningful public scrutiny of election processes, which can assist with the detection of improper physical access of election assets or malicious cyber activity

Speaking: Jennifer Morrell, CISA Election Security Expert Consultant

Tell: What You Can Tell Your Voters

Processes and Procedures (Track)

- Clear communications around election administration can help manage significant and persistent risks of MDM
- What process and procedure documents are worth sharing?
- Consider augmenting communication around processes that voters may have diminished trust in

Examples of processes to track

- Secure mail ballot processing procedures
- Rigorous voter verification and signature verification procedures
- Voter registration list maintenance procedures
- Voting equipment testing and security procedures

Test & Audit Results (Test)

- Providing information that your best practices are followed can minimize the risks of MDM catching hold
- Being transparent by involving the public allows them to verify the testing and results on their own

Examples of results to provide

- Compliance audits (SOPs, security, chain of custody)
- L&A test results (Pre- & Post-election L&A)
- Ballot reconciliation logs and forms
- Ballot manifests
- Post-election tabulation audit results

Speaking: Jennifer Morrell, CISA Election Security Expert Consultant

Tell: How to Set Public Expectations

Clear communication around public expectations

- Important dates both pre- and post Election Day
- Historical turnout data for like elections
- Voter registration trends since last like election
- Schedule of when results will be released (stress that counting is never completed on Election Day)
  - Stay on schedule, do not post updated results off-schedule
  - Depending on frequency, you may see large updates (spikes) to results well after closing of polls on election night.
  - Stress that until all ballots are counted, results will change, and outcomes may change until final certification
- Any variation to the above should be communicated broadly and immediately
- Provide as much transparency as possible on voter numbers and update them regularly (e.g., number of registered voters; number of mail-ballots requested, transmitted to voters, returned; number of early in-person voters; etc.)

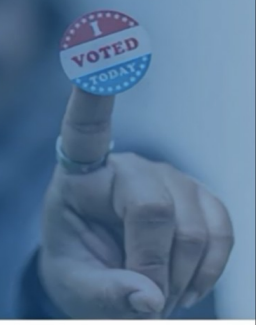
Engage the public in the process – encourage public participation

- When feasible, testing and auditing should be open to the public
- Encourage bi-partisan participation
- Use the opportunity to educate the public
- Allow for inspection of SOPs, testing logs, audit reports, etc.
- Publicly stream the process so voter can watch from afar and at their convenience

Speaking: Jennifer Morrell, CISA Election Security Expert Consultant

Tell: Tools for Telling Your Story

- **Encourage in-person observation (building team of validators)**
- **Use election stakeholders to help spread accurate information**
- **Build civic and government partnerships**
- **Conduct community town halls (in-person or virtual)**
- **Strengthen relationships with earned media (local news, radio, newspapers, etc.)**
- **Post educational videos of your processes**
- **Perform facility tours to explain election security measures and processes (in-person or virtual)**
- **Visually present process maps**
- **Livestream your activities**
- **Distribute important information via social Media (pay for targeted messaging)**



Speaking: Jennifer Morrell, CISA Election Security Expert Consultant

Tell: When MDM Impacts Your Operation

- Engage trusted voices
- Communicate without amplifying the MDM narrative
- Lead with the truth, not the rumor
- Restate the fact again
- Keep it simple
- Be consistent in your choice of MDM narratives to debunk



Speaking: Jennifer Morrell, CISA Election Security Expert Consultant

26

Secure Practices

Enhance election security practices to decrease the likelihood of operational mistakes, build trust through secure practices, and protect systems, data, and personnel.

Building Trust Through Secure Practices

- **Isolated errors and confusion** can feed destructive narratives.
- **Public misunderstanding of processes** allows MDM to grow and thrive.
- **MDM undermines confidence and trust** in elections.
- You can't stop MDM, but you can mitigate its impact by **sharing relevant facts.**

What Can Election Officials Do?

- **Track:**
  Document your cybersecurity, physical security, and operational security processes and procedures to ensure that safeguards are enacted and implemented.
- **Test:**
  Verify and audit your processes and procedures, the work of your staff, and the functioning of election infrastructure.
- **Tell:**
  Provide fact-based evidence of why your voters should trust elections and get ahead of likely stories by pre-bunking false narratives before they catch hold, and then quickly rebutting them if they do start to spread.

What is MDM?

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

Three T's: Track, Test, Tell




As the nation's risk advisor, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the security and resiliency of our critical infrastructure.
CISA provides training, resources, and tools to harden security postures and mitigate potential issues. Contact CISA at Central@CISA.gov for assistance with:
Physical Security
Protective Security Advisors (PSAs) provide facility walkthroughs and recommendations
Cybersecurity
Cybersecurity Advisors (CSAs) conduct site visits to discuss protection of networks and systems access control as a defense of networks and devices
Provide assessment on systems to identify vulnerabilities
Provide incident response planning support
MDM
Guidance on how critical infrastructure-related misinformation, disinformation, and malinformation can spread, and what signs to watch for
Visit cisa.gov/election-security to learn about CISA's role in election security.
Track
Create documentation to detail both how security practices should be conducted and how they are being conducted through robust chain-of-custody and physical security procedures.
Written Standard Operating Procedures (SOPs) should be extensively detailed. Provide sequential steps and include visual depictions, examples, checklists, and forms for verification.
Asset tracking and access control for systems, people, documents, and data transactions should be implemented and logged. Automating the process can make it easier to capture what is happening and when.
Control forms– including chain-of-custody documentation, ballot duplication logs, and election night reporting uploads– capture data with precision at critical points to provide evidence for audits or incident analysis.
Test
Verify the work of staff and the functioning of election assets and processes with robust testing and auditing.
Conduct post election tabulation audits by reviewing a sample of voted ballots against the voting machine records to ensure accuracy.
Informal compliance audits ensure SOPs work. Formal compliance audits ensure SOPs are being followed.
Test processes to ensure chain of custody on your critical assets is never broken and that you have the evidence to prove it.
Tell
Convince voters to trust elections with proactive and responsive fact-based communication and transparency measures.
Election officials are the absolute authority on election administration.
Clear communication around election administration can help manage the significant and persistent risks of MDM.
Use documentation from your Tracking and Testing practices as communication content to share information.
Engage the public in the process– encourage public participation.


CISA
CYBER+INFRASTRUCTURE
David Kuennen
Team Lead, Engagement, Assistance, and Training
Election Security Initiative
david.kuennen@cisa.dhs.gov
Jennifer Morrell and Noah Praetz
Subject Matter Expert Consultant, Election Security
Election Security Initiative
electionsecurity@cisa.dhs.gov
Contact CISA:
Central@cisa.dhs.gov
Speaking: Noah Praetz, CISA Election Security Expert Consultant
CISA
January 17, 2022
30

From: Holmes, Stuart <stuart.holmes@sos.wa.gov>
Subject: [SUSPICIOUS] Revision to WAC 434-335-260
To:
Cc: Hunt, Heidi (Adams County) <heidih@co.adams.wa.us>; Darla McKay(dmckay@co.asotin.wa.us) <dmckay@co.asotin.wa.us>; Chilton, Brenda (BentonCounty) <Brenda.Chilton@co.benton.wa.us>; Moore, Skip (Chelan County) <Skip.Moore@CO.CHELAN.WA.US>; Shoona Riggs (sriggs@co.clallam.wa.us) <sriggs@co.clallam.wa.us>; Kimsey, Greg (Clark County) <Greg.Kimsey@clark.wa.gov>; Anne Higgins (anne_higgins@co.columbia.wa.us) <anne_higgins@co.columbia.wa.us>; Elliott, David <david.elliott@sos.wa.gov>; Carolyn Fundingsland(FundingslandC@co.cowlitz.wa.us) <FundingslandC@co.cowlitz.wa.us>; ThadDuvall (tduvall@co.douglas.wa.us) <tduvall@co.douglas.wa.us>; DiannaGalvan (auditor@co.ferry.wa.us) <auditor@co.ferry.wa.us>; Matt Beaton(mbeaton@co.franklin.wa.us) <mbeaton@co.franklin.wa.us>; McKenzie Lueck -Garfield (mlueck@co.garfield.wa.us) <mlueck@co.garfield.wa.us>; JoeMacLean (JMacLean@co.grays-harbor.wa.us) <JMacLean@co.grays-harbor.wa.us>; Sheilah Crider - Island (S.Crider@islandcountywa.gov) <S.Crider@islandcountywa.gov>; Rose Ann Carroll(carrollra@co.jefferson.wa.us) <carrollra@co.jefferson.wa.us>; Wise, Julie(King County) <Julie.Wise@kingcounty.gov>; Paul Andrews(pandrews@co.kitsap.wa.us) <pandrews@co.kitsap.wa.us>; Jerry Pettit(jerry.pettit@co.kittitas.wa.us) <jerry.pettit@co.kittitas.wa.us>; BrendaSorensen (brendas@klickitatcounty.org) <brendas@klickitatcounty.org>; Larry Grove (larry.grove@lewiscountywa.gov) <larry.grove@lewiscountywa.gov>; Chandra Schumacher(cschumacher@co.lincoln.wa.us) <cschumacher@co.lincoln.wa.us>; PaddyMcGuire (pmcguire@co.mason.wa.us) <pmcguire@co.mason.wa.us>; Cari Hall(chall@co.okanogan.wa.us) <chall@co.okanogan.wa.us>; Joyce Kidd(jkidd@co.pacific.wa.us) <jkidd@co.pacific.wa.us>; Marianne Nichols(mnichols@pendoreille.org) <mnichols@pendoreille.org>; Julie Anderson -Pierce (julie.anderson@piercecountywa.gov) <julie.anderson@piercecountywa.gov>; Milene Henley (mileneh@sanjuanco.com) <mileneh@sanjuanco.com>; Sandra Perkins - Skagit (sandyp@co.skagit.wa.us) <sandyp@co.skagit.wa.us>; Robert Waymire (rwaymire@co.skamania.wa.us) <rwaymire@co.skamania.wa.us>; Garth Fell (garth.fell@co.snohomish.wa.us) <garth.fell@co.snohomish.wa.us>; Dalton, Vicky (Spokane County) <VDalton@spokanecounty.org>; llarsen@stevenscountywa.gov <llarsen@stevenscountywa.gov>; Mary Hall <mary.hall@co.thurston.wa.us>; Nicci Bergseng <bergsengn@co.wahkiakum.wa.us>; Karen Martin(kmmartin@co.walla-walla.wa.us) <kmmartin@co.walla-walla.wa.us>; DianaBradrick (dbradric@co.whatcom.wa.us) <dbradric@co.whatcom.wa.us>; SandyJamison (sandy.jamison@co.whitman.wa.us) <sandy.jamison@co.whitman.wa.us>; Charles Ross (charles.ross@co.yakima.wa.us) <charles.ross@co.yakima.wa.us>; Ormond, Fina <fina.ormond@sos.wa.gov>
Sent: March 16, 2022 3:29 PM (UTC-04:00)
Attached: Clearinghouse - Access to Voting System.docx, WAC 434-335-260.docx

Distribution: County Auditors

Good afternoon,

Attached is a proposed revision that I drafted for WAC 434-335-260 regarding decertification of voting systems. I've also included a draft Clearinghouse that would be a companion document for this WAC. I believe this qualifies for emergency adoption of this WAC to protect the security of the voting system. I believe this combination of WAC and Clearinghouse simply puts into writing what is already being done in practice. However, it provides clarity of the impacts on unauthorized access to a voting system.

I'm coordinating this call to go over the proposed changes, answer any questions, gather any constructive feedback and useful clarifications on the draft WAC or Clearinghouse before they're adopted. I apologize for the short notice.

WASHINGTON SECRETARY OF STATE

Elections Division

Access to Voting System Software and Systems

Elections Clearinghouse Notice
Issue #
March 14, 2022

Background

The Office of the Secretary of State has duties, pursuant RCW 29A.12.020, to inspect, evaluate, and publicly test all voting systems or components of voting systems. These reviews include verifying that the voting system conforms to federal and state law and any regulations or standards regarding confidentiality, security, accuracy, safety, reliability, usability, accessibility, durability, resiliency, and auditability. This is in addition to the Federal testing and certification by an independent testing authority designated by the United States Election Assistance Commission (EAC).

The Help America Vote Act (HAVA) of 2002 was passed by the United States Congress to make sweeping reforms to the nation's voting process. HAVA also established the Election Assistance Commission (EAC) to assist the states regarding HAVA compliance and to distribute HAVA funds to the states. EAC is also charged with creating voting system guidelines and operating the federal government's first voting system certification program. On December 13, 2005, the EAC unanimously adopted the 2005 Voluntary Voting System Guidelines (VVSG), which significantly increased security requirements for voting systems and expanded access, including opportunities for individuals with disabilities to vote privately and independently.

In January 2017, the U.S. Department of Homeland Security designated election infrastructure as critical infrastructure under the "Government Facilities" sector, one of the 16 critical infrastructure sectors in the United States.

Third-Party Access to Voting Systems.

Demands have been made to allow third-party entities not directly involved with the conduct of elections to have access to electronic voting systems, specifically to review and copy the internal electronic, software, mechanical, logic, and related components of such systems. These demands have included the desire to image electronic memory spaces, to download operating systems and software, and to copy information that is internal and proprietary. Such access by third parties undermines chain of custody requirements and strict access limitations necessary to prevent both intentional and inadvertent tampering with electronic voting systems.

It also jeopardizes the security and integrity of those systems and will negate the ability of electronic voting system vendors to affirmatively state that such systems continue to meet security standards, are validated as not posing security risks, and are able to be certified to perform as designed by the

electronic voting system vendor and as certified by both the U.S. Election Assistance Commission and the Office of the Secretary of State.

Limits on Third-Party Access to Electronic Voting Systems.

WAC 434-335-260 has been amended to clarify that:

a. County Auditors shall not provide physical, electronic, or internal access to third parties seeking to copy and/or conduct an examination of state-certified voting systems, or any components of such systems, including but not limited to: election management software and systems, tabulators, scanners, counters, automatic tabulating equipment, voting devices, servers, ballot marking devices, paper ballot printers, portable memory media devices (thumb drives, flash drives and the like), and any other hardware, software or devices being used as part of the election management system.

b. If access described in a. occurs, those pieces of voting equipment will be considered no longer secure or reliable to use in subsequent elections. As a result, the Office of the Secretary of State will decertify the use of the system or component. Additionally, incidents will be treated as a security breach under RCW 29A.12.180.

Voting System Replacement Costs

The Office of the Secretary of State may not reimburse the cost of replacement voting equipment for which unauthorized access was granted.

Notice

County Auditors shall notify the Secretary immediately upon receipt of any written or verbal request for third-party access to a voting system, or any component thereof.

In addition, County Auditors and voting system vendors are required by RCW 29A.12.180 to disclose of any breach or attempted breach in the chain of custody of its voting system components.

WAC 434-335-260

Decertification of voting systems and vote tabulating systems.

(1) The secretary of state may decertify a voting system or vote tabulating system or any component thereof and withdraw authority for its future use or sale in Washington if, at any time after certification the secretary of state determines that:

(a) The system or component fails to meet the standards set forth in applicable federal guidelines or state statutes or rules;

(b) The system or component was materially misrepresented in the certification application; or

(c) The applicant has installed unauthorized modifications to the certified software or hardware. ; or

(d) The system or component was operated or accessed in Washington State at any time by anyone other than an authorized staff member of the office of the secretary of state, an authorized staff member of the county auditor's office, for the purposes of maintenance and operation under RCW 29A.12.060, an independent testing authority designated by the United States election assistance commission, or an independent testing authority and the test plan has received approval by both the county auditor and secretary of state.

(2) The secretary of state must provide written notice of intent to decertify to the original applicant or its successor, if known, to all county auditors, and to the public. The notice must specify the reasons why the certification of the system may be rescinded. The applicant or successor or any county auditor may, within thirty days after the issuance of the notice, file with the secretary of state a written explanation as to why the system or component should not be decertified. The secretary of state may extend or shorten the time for filing of a written explanation for good cause. After reviewing the explanation, the secretary of state may either discontinue the decertification process, in which case the system or component remains certified, or schedule a public hearing pursuant to subsection (3) of this section. If no explanation is timely filed, the secretary of state may either discontinue the decertification process or issue a final order pursuant to subsection (4) of this section.

(3) A decertification proceeding shall constitute an adjudicative proceeding pursuant to chapter **34.05** RCW.

(a) The secretary of state adopts the model rules of procedure as set forth in chapter **10-08** WAC, except as they may be inconsistent with this chapter. The proceeding may be conducted as an emergency adjudicative proceeding pursuant

to RCW **34.05.479** if the secretary of state finds that immediate action is required to preserve the integrity of the electoral process.

(b) The secretary of state shall designate the presiding officer.

(c) The certification remains valid pending resolution of the administrative proceeding, unless the secretary of state finds, following notice and opportunity for written or oral input, which may be expedited, that the public interest requires that the decertification should take effect on a temporary basis pending hearing.

(d) The argument in favor of decertification may be presented by an employee of the secretary of state or by an assistant attorney general. Other parties may be represented by a certified election administrator or by any person permitted to appear by ~~WAC 434-180-560~~the county auditor.

(4) The presiding officer or secretary shall enter an order specifying the system or component at issue, whether or not it is decertified, the effective date of any decertification, and explain the basis for the decision. The effective date of decertification shall not be less than five days after the entry of the order, but may be delayed to any reasonable date. An order issued by the secretary pursuant to subsection (2) of this section is a final order. An order issued by the presiding officer is regarded as an initial order unless the secretary of state, assistant secretary of state, deputy secretary of state, or director of elections presides, in which case the decision of the presiding officer shall be final and no further review is available within the agency.

[Statutory Authority: RCW **29A.04.611**. WSR 05-18-022, § 434-335-260, filed 8/29/05, effective 9/29/05.]

The cumulative effect of these state policies and administrative actions is far more consequential than procedural violations or individual failures of governance. They represent a coordinated effort to institutionalize a culture of opacity, shield election systems from public accountability, and undermine the critical infrastructure mandates designed to protect the integrity of elections. This deliberate evasion of federal requirements, such as those outlined in **EO 13800** and the **NIST Cybersecurity Framework**, demonstrates not only negligence but also a systemic intent to bypass mechanisms of oversight and transparency.

The refusal to allow third-party compliance testing, codified in the **WAC** amendments and enforced through the **Clearinghouse notice,** cannot be viewed in isolation. It is part of a larger strategy to centralize control within a tightly restricted administrative framework, preventing external audits and accountability while consolidating authority under state actors like **Stuart Holmes** and the **Secretary of State**. This raises critical concerns about the unchecked power of unelected officials and the legislative complicity in facilitating such overreach. By designating third-party assessments as breaches of the chain of custody, these policies conflate necessary security measures with procedural obstructionism, masking their intent to sidestep federal law.

At its core, this issue transcends the boundaries of election security and ventures into the erosion of democratic principles. Transparency in elections is not merely a procedural safeguard—it is a cornerstone of public trust and confidence in the democratic process. By systematically denying access to cast vote records, obstructing compliance testing, and insulating election systems from independent oversight, these actions strike at the heart of what it means to have free and fair elections. The implications extend beyond Washington State, setting a dangerous precedent for other states to follow similar paths, thereby nationalizing a framework of secrecy and unaccountability.

The use of imprinting systems on ballots and envelopes, combined with advanced chain-of-custody protocols, exemplifies this duality of intent. These measures are marketed as enhancements to security and transparency, yet their practical application has created a system where voter privacy is compromised, and public access to critical election records is denied. The integration of such technologies into risk-limiting audits (RLAs) further complicates the narrative, as the very systems designed to enhance accuracy and security also facilitate secrecy and centralization.

Beyond the administrative and legislative maneuvers, there is an inherent conflict in the delegation of election responsibilities. By relying on federal advisory bodies like **CISA** and the **EAC**, **Washington's** election officials have undermined state sovereignty and allowed federal influence to dictate processes that are constitutionally reserved for the states. This conflict reflects a broader trend in the nationalization of election security—a trend that undermines the decentralization of power and the checks and balances necessary to prevent systemic abuses.

The actions of state officials, including legislators, the **Secretary of State,** and unelected administrators like **Stuart Holmes**, should be evaluated not only in terms of their immediate impact but also in the context of their long-term consequences. These individuals are not merely administrative stewards; they are custodians of public trust, with responsibilities that extend to the protection of democratic integrity and the rule of law. The erosion of these principles underlines the gravity of their failures and the urgent need for systemic accountability.

This accountability is not optional—it is an imperative grounded in the **Constitution** and federal law. While the legal frameworks are clear, the intentional subversion of these frameworks demonstrates a level of malfeasance that requires redress. The consequences of such actions are not confined to administrative penalties or procedural corrections; they fundamentally threaten the legitimacy of the electoral process and the democratic institutions it supports.

The resistance to transparency and accountability in **Washington's** election system extends to even the formal processes outlined by state officials. In **Clark County,** election integrity advocates formally requested a full forensic audit from **County Auditor Greg Kimsey**. Acting in accordance with **Stuart Holmes' Clearinghouse notice,** which requires county auditors to report all such requests, **Kimsey** asked for the request to be submitted in writing. This allowed him to fulfill his obligation to notify the **Washington State Association of County Auditors (WSACA)**, which escalates these matters to the unelected elections director, Stuart Holmes. The response to this written request, as documented in the email exchange, demonstrates the systemic effort to avoid meaningful transparency while redirecting such demands toward narrow alternatives, such as risk-limiting audits, that align with the restrictive framework imposed by **Holmes** and the **OSOS.**

From: Greg Kimsey <Greg.Kimsey@clark.wa.gov>
Subject: Election Integrity Committee report
To: Dianna Galvan <auditor@co.ferry.wa.us>; Anne Higgins - Columbia <anne_higgins@co.columbia.wa.us>; Brenda Chilton <brenda.chilton@co.benton.wa.us>; Brenda Sorensen <brendas@co.klickitat.wa.us>; Cari Hall <chall@co.okanogan.wa.us>; CarolynFundingsland <FundingslandC@co.cowlitz.wa.us>; Carolyn Weikel <Carolyn.Weikel@snoco.org>; Charles Ross <charles.ross@co.yakima.wa.us>; Darla McKay <dmckay@co.asotin.wa.us>; Diana Bradrick <DBradric@co.whatcom.wa.us>; Dolores Gilmore <dgilmore@co.kitsap.wa.us>; Garth Fell <garth.fell@co.snohomish.wa.us>; Heidi Hunt - Adams <heidih@co.adams.wa.us>; Huff, Sherril <sherril.huff@kingcounty.gov>; Jerry V. Pettit <jerry.pettit@co.kittitas.wa.us>; Joe MacLean <JMacLean@co.grays-harbor.wa.us>; Joyce Kidd <jkidd@co.pacific.wa.us>; Julie Anderson <julie.anderson@co.pierce.wa.us>; Karen Martin <kmmartin@co.walla-walla.wa.us>; Larry Grove <larry.grove@lewiscountywa.gov>; Lori Larsen - Stevens <llarsen@stevenscountywa.gov>; Marianne Nichols <mnichols@pendoreille.org>; Mary Hall <mary.hall@co.thurston.wa.us>; MattBeaton <mbeaton@co.franklin.wa.us>; McKenzie Lueck <mlueck@co.garfield.wa.us>; Michele Jaderlund <mjaderlund@grantcountywa.gov>; Milene Henley - San Juan <mileneh@co.san-juan.wa.us>; Nicci Bergeseng <bergsengn@co.wahkiakum.wa.us>; Paddy Macguire <pmcguire@co.mason.wa.us>; Paul Andrews <PaulAndrews@co.kitsap.wa.us>; Robert Waymire <rwaymire@co.skamania.wa.us>; Rose Ann Carroll <racarroll@co.jefferson.wa.us>; Sandy Jamison <auditor@co.whitman.wa.us>; Sandy Perkins <sandyp@co.skagit.wa.us>; Sheilah Crider <S.Crider@islandcountywa.gov>; Shelly Johnston <sjohnston@co.lincoln.wa.us>; Shoona Riggs <sriggs@co.clallam.wa.us>; Skip Moore <Skip.Moore@CO.CHELAN.WA.US>; Thad Duvall <tduvall@co.douglas.wa.us>; TimTodd <todd@co.skamania.wa.us>; Vicky Dalton <vdalton@spokanecounty.org>
Sent: March 4, 2022 3:28 PM (UTC-05:00)
Attached: CCRP EIT In Writing Request for FFEA to CC Auditor.docx

Good afternoon, I am providing you the attached document at the request of the authors of that document. I am willing to lead a discussion of the contents of that document.

Regards,
Greg

Clark County Republican Party Election Integrity Team's Response to Clark County Auditor's July 9, 2021 Request to 'Put It In Writing'

Clark County WA Auditor: Request For Full Forensic Kinematic Election Audit of the November 3, 2020 Election

Full Forensic Election Audit Actions Requested of Clark County Auditor

1. Agree to facilitate the CLARK COUNTY WA CITIZENS' REQUEST FOR A FULL FORENSIC ELECTION AUDIT OF THE Nov. 3, 2020 General Election acknowledging this is a good faith request to restore public confidence in our sacred Elections and to restore 'Equal Protection Under the Law' for all voters here in Clark County WA since that protection has been and is currently being violated. All of the following examples below violate USA and WA State legal voting citizens' Equal Protection Under the Law.

    a. Illegal Aliens Registering and Voting.
    b. Inaccurate Registered Voter Lists.
    c. Illegal vendor upgrades to voting machine software, operating systems, voting system applications, and hardware without performing and archiving the required (before and after) system image backups, (WIN 7 to WIN 10 and Hart Verity 2.3 to 2.5).
    d. No permanent residency verification 30 days prior to election day for persons registering to vote.
    e. Allowing Clark County Jail inmates to register and vote while incarcerated without felony or misdemeanor verification, no USA Citizenship verification, and no Clark County 30 day residency requirement verification.
    f. Inadequate and untimely voter registration roll maintenance – verification requirements not done until after election is 'certified' if then.
    g. Insufficient cross checking with all 50 States, D.C., and US Territories for duplicate, deceased, illegal alien, and felon voters prior to registering voters and allowing them to vote.
    h. No photo identification requested from persons requesting to register to vote.
    i. No proof of US Citizenship requested from persons requesting to register to vote at Elections Department nor DOL.
    j. No proof of 30 day permanent residency requested from persons requesting to register to vote.
2. Agree to provide all Nov. 3, 2020 General Election Paper Ballots and all associated documents to the Audit Team.

3. Agree to implement all recommendations of the Audit Team that are demonstrably constructive, accurate, and deemed necessary to restore public confidence in voter and election integrity, security, and overall chain of custody adherence here in Clark County, WA.
4. Agree to lobby for and persuade WA State Legislature (especially Clark County Representatives, Senators, and candidates) to propose and pass Election Integrity legislation deemed critical for the entire state to adopt, pass, and implement to be in place/ready for the 2022 Midterm Elections with requests to Secretary of State for concurrent support of the same.
5. Provide a signed copy of your oath of office to the Audit team.
6. Please indicate your understanding and concurrence with the following?
    a. *"How can we possibly believe that our elections are secure and that there is no possibility of widespread fraud if election Full Forensic Audits have never been performed?"*
7. Acknowledge receipt of this document and respond in writing within 5 working days of being served this request.

Full Forensic Election Detailed Audit Steps Requesting Clark County Auditor to Agree To

1. Meet with the Clark County Republican Party Election Integrity Team to discuss and agree to the Full Forensic Election Audit Team's scope of work, establish a mutually agreeable time interval, media/press reporting protocol, as well as preliminary, and final AUDIT TEAM reporting protocols.
2. Provide immediate access to the stored Nov. 3, 2020 General Election Ballots to enable commencement of a HAND RECOUNT of Paper Ballots
3. Provide in writing cost estimates of Elections Dept. Staff/Support Personnel to Audit Team based on the scope of work provided herein.
4. Provide all HART INTER-CIVIC Verity documentation to Audit Team and their Designated Contractor Representatives (Cyber Ninjas / other for example)
5. Provide Clark County Elections Staff (Richard Cooper Specifically) access & time to consult with the Audit Team regarding Clark County Elections Dept. Hart machinery settings used on the Nov. 3, 2020 General Election. (Example – Verity Release 2.3 vs. current upgraded version of 2.5)
6. Provide access to all Hart Equipment by Audit Team and their digital contractors along with all correspondence related to the Hart Inter-Civic Contract.
7. Provide all election machinery certifications from Voting System Test Laboratories leading up to and including the Nov. 3, 2020 General Election.
    - Voting System Test Laboratories (VSTL) | U.S. Election Assistance Commission (eac.gov)
8. Agree in written response to make yourself and your staff available to the Audit Team during 8 AM-5 PM normal working hours for on call and in person questions from the Audit Team including DID (direct inward dial) phone numbers, email addresses, and cell numbers - including personal cell numbers.
9. Provide Audit Team all Clark County & Secretary of State Elections Departments policies, directives, executive orders, and directions (both written and verbal understandings) from Secretary of State and from yourself to your staff on exactly how they are to interpret and process voter registration requests and elections given WA STATE RCW and WAC s in light of the superiority of WA STATE CONSTITUTION Election wording of Common Law. This is especially critical with the high rate of illegal aliens coming to WA state due to the unconstitutional illegal open border policies of the Biden Administration and WA State's unconstitutional 'sanctuary state' status.
10. Review and provide your comments on all seven tabbed sub-categories
    - Mail-in Fraud - 2020 Election Irregularities
11. Please understand and acknowledge that we the people rely on duly elected officials like yourself to guard and protect our civil rights as legal USA citizens' voters - especially our right to EQUAL PROTECTION UNDER THE LAW for our legal votes - as mandated by the USA and WA State Constitutions as well as US Common Law. RCW 4.04.010

- Common law is a body of unwritten laws based on legal precedents established by the courts. Common law influences the decision-making process in unusual cases where the outcome cannot be determined based on existing statutes or written rules of law. The U.S. common-law system evolved from a British tradition that spread to North America during the 17th and 18th century colonial period.

12. Please indicate how you as Clark County Auditor will provide remedies to all legal USA Citizen voters of Clark County WA who are now demanding restoration of our EQUAL PROTECTION UNDER THE LAW – for our votes and our elections. Two examples would be establishment of election worker teams that are bipartisan in nature (vs. unknown) and discontinuing spousal team workers.

Full Forensic Audits Reference – 'No' on your/SOS recent suggestion/offering to conduct a RLA (Risk Limited Audit). This is an unacceptable solution offering per your recent suggestion.

- Full Forensic Audits vs. Superficial Recounts - UncoverDC

The team stated that the three objectives of meaningful election audits are:

> (a) to identify and fix honest mistakes,
>
> (b) to detect evidence of malfeasance, and
>
> (c) to maintain/restore public confidence in the outcome of an election.

The three major elements of an election that can go wrong are:

> 1 – the Voter,
>
> 2 – the Machine (voting System Equipment), and
>
> 3 – the ballot Process.

In an FFA, each of these areas would be thoroughly analyzed to determine such things as:

> 1 – Did only legally eligible citizens vote, and just once?
>
> 2 – Did the voting machines accurately report all ballots received, without any changes?
>
> 3 – Did third parties illegally change or delete any legitimate ballots, or add ballots?

The outright denial of third-party audits of voting machines in **Washington State** is not just a technical or procedural failure—it is a deliberate and systemic policy that directly contravenes federal cybersecurity mandates and undermines public trust in elections. The actions of state officials, as demonstrated by their written refusals and the administrative frameworks they have implemented, reveal an entrenched resistance to transparency and accountability.

At the heart of this issue is the amendment to **WAC 434-335-260**, which explicitly prohibits third-party assessments of voting systems. This restriction, codified under the guise of protecting chain-of-custody integrity, effectively shields these systems from the independent scrutiny required to ensure compliance with federal cybersecurity standards. The irony here is stark: while the officials claim that allowing third-party audits would compromise security, these audits are precisely what federal frameworks like the **NIST Cybersecurity Framework (CSF)** and **EO 13800** prescribe to secure critical infrastructure.

The refusal to permit third-party audits is further exemplified in the written responses from county auditors, such as the documented interaction in **Clark County**. Election integrity advocates followed the formal procedure to request a forensic audit, only to be met with a refusal and an offer to conduct a risk-limiting audit (RLA) instead. This substitution is emblematic of the broader issue: RLAs are tightly controlled processes that rely on systems designed to centralize and obfuscate rather than open the election process to independent validation. The offer of an RLA in lieu of a forensic audit represents not a solution but a perpetuation of the very opacity that undermines election security.

Moreover, the **Clearinghouse notice** issued by **Stuart Holmes** compounds this issue by requiring county auditors to immediately report any verbal or written requests for third-party audits. This directive creates an environment of preemptive denial, where the default response to such requests is rejection rather than engagement. The narrative that third-party audits breach chain-of-custody protocols is a misrepresentation of the role these audits play in enhancing security, as compliance testing occurs before elections, not during the handling of active ballots. This misrepresentation is a clear strategy to evade oversight and prevent the public from accessing critical information about the security and functionality of election systems.

The refusal to allow third-party audits has far-reaching implications beyond the borders of **Washington State**. It sets a dangerous precedent for other states to follow similar paths, eroding the principles of transparency and public accountability that are foundational to democratic governance. By insulating voting systems from independent scrutiny, state officials are not only violating federal mandates but also exposing these systems to unmitigated vulnerabilities that could compromise the integrity of elections.

Ultimately, the denial of third-party audits is a direct affront to the very principles of election security that officials claim to uphold. It underscores the need for robust federal oversight and enforcement to ensure that states comply with the mandates designed to protect critical infrastructure. Without such measures, the public's faith in the electoral process will continue to erode, leaving the democratic institutions it supports increasingly vulnerable.

The systemic resistance to third-party audits and transparency in **Washington's** election processes is not limited to county-level requests. Even state legislators advocating for heightened accountability and forensic imaging of election systems have faced outright denials. **Representative Vicki Kraft's** formal request for forensic imaging of all election systems prior to any software or hardware upgrades following the 2020 election underscores the growing demand for independent verification at all levels of government. The response from then-**Secretary of State Kim Wyman,** dismissing the request on the grounds of lacking legislative or administrative precedent, exemplifies the institutional barriers erected to block meaningful scrutiny. This exchange further illustrates the state's entrenched position against independent assessments, even when federal law explicitly supports such measures.

From: Kraft, Rep. Vicki [mailto:Vicki.Kraft@leg.wa.gov]

Sent: Tuesday, August 17, 2021 9:37 AM

To: Wyman, Kim (Web) ; Hunt, Heidi (Adams County) ; dmckay@co.asotin.wa.us; Chilton, Brenda (Benton County) ; Moore, Skip (Chelan County) ; sriggs@co.clallam.wa.us; Kimsey, Greg (Clark County) ; anne_higgins@co.columbia.wa.us; fundingslandc@co.cowlitz.wa.us; tduvall@co.douglas.wa.us; auditor@co.ferry.wa.us; mbeaton@co.franklin.wa.us; mlueck@co.garfield.wa.us; mjaderlund@grantcountywa.gov; jmaclean@co.grays-harbor.wa.us; s.crider@islandcountywa.gov; racarroll@co.jefferson.wa.us; Wise, Julie (King County) ; pandrews@co.kitsap.wa.us; jerry.pettit@co.kittitas.wa.us; brendas@klickitatcounty.org; larry.grove@lewiscountywa.gov; rluiten@co.lincoln.wa.us; skf@masoncountywa.gov; chall@co.okanogan.wa.us; jkidd@co.pacific.wa.us; mnichols@pendoreille.org; julie.anderson@co.pierce.wa.us; mileneh@sanjuanco.com; sandyp@co.skagit.wa.us; rwaymire@co.skamania.wa.us; Garth.Fell@snoco.org; Dalton, Vicky (Spokane County) ; llarsen@stevenscountygov.wa; hallm@co.thurston.wa.us; bergsengn@co.wahkiakum.wa.us; kmmartin@co.walla-walla.wa.us; Dbradric@co.whatcom.wa.us; auditor@co.whitman.wa.us; Charles.Ross@co.yakima.wa.us

Cc: @SRC Members ; @SDC Members ; @HRC Members ; @HDC Members

Subject: Letter requesting: Forensic image before Nov. 2020 election systems upgrades

Secretary Wyman and the 39 WA County Auditors –

Please see the letter below, which is also attached.

STATE REPRESENTATIVE
17th LEGISLATIVE DISTRICT
VICKI KRAFT

Washington
House of
Representatives

CAPITAL BUDGET
COLLEGE & WORKFORCE DEVELOPMENT
COMMUNITY & ECONOMIC DEVELOPMENT

August 17, 2021

Secretary Kim Wyman
Office of the Secretary of State
P.O. Box 40220
Olympia, WA 98504-0220

Washington County Auditors
Of all 39 Counties in WA State

ELECTRONIC DELIVERY

Secretary Wyman and Washington County Auditors:

As you're aware, there are many people across our state who are very concerned about the integrity of our Washington election processes and the outcome of those processes in the November 2020 election. Washington state has been using election processes for years, which were determined during the last election, to be practices ripe for fraud when other states (PA, GA, etc.) tried to implement them – mail-in voting, early voting, counting ballots after the election date, ballot harvesting, same day voter registration, etc. Clearly there are many questions and issues to be addressed regarding our November 2020 elections.

I am writing to request and demand that a forensic image of any and every election system in each county, especially any used in the November 2020 election, be properly captured before any upgrade (software, hardware, etc.) is done. A backup is not the same as a forensic image. Capturing a forensic image of these systems will work to help ensure the integrity of the system before and after the upgrade. It will also provide the proper information needed in the case of a forensic audit.

If you have, or have not, already captured a forensic image of your election systems before making any upgrades following the November 2020 election, please let me know this. I am also requesting you respond to me to advise of

LEGISLATIVE OFFICE: 436 JOHN L. O'BRIEN BUILDING • PO BOX 40600 • OLYMPIA, WA 98504-0600 • 360-786-7994

your forensic imaging process and retention policy for digital and paper election records. You are welcome to respond to the entire Legislature as well, whom I have copied on the electronic delivery of this letter.

Federal Code Title 52 USC 20701 requires all records and papers related to an election be retained and preserved for a period of twenty-two months. This requires all digital records and data as well. Taking a forensic image of all election systems before any upgrade is completed will help ensure the optimum integrity of these records.

This is not a partisan issue. We all have the duty of providing the highest level of integrity, transparency and accountability when executing the duties of our office. As the election officials for our state, you have a critical role and responsibility in ensuring all properly registered Washington voters can have confidence their vote and voice was accurately counted. Your help with this request will work to achieve that essential outcome.

Thank you in advance, for your assistance with this important matter.

Sincerely,



Representative Vicki Kraft

17th Legislative District

From: Public Records <publicrecords@sos.wa.gov>
Subject: FW: Letter requesting: Forensic image before Nov. 2020 election systems upgrades
To: Vicki.Kraft@leg.wa.gov <Vicki.Kraft@leg.wa.gov>
Cc: Wyman, Kim (Web) <kim.wyman@sos.wa.gov>; Hunt, Heidi (Adams County) <heidih@co.adams.wa.us>; dmckay@co.asotin.wa.us <dmckay@co.asotin.wa.us>; Chilton, Brenda (Benton County) <Brenda.Chilton@co.benton.wa.us>; Moore,Skip (Chelan County) <Skip.Moore@CO.CHELAN.WA.US>; sriggs@co.clallam.wa.us <sriggs@co.clallam.wa.us>; Kimsey, Greg (Clark County) <Greg.Kimsey@clark.wa.gov>; anne_higgins@co.columbia.wa.us <anne_higgins@co.columbia.wa.us>; fundingslandc@co.cowlitz.wa.us <fundingslandc@co.cowlitz.wa.us>; tduvall@co.douglas.wa.us <tduvall@co.douglas.wa.us>; auditor@co.ferry.wa.us <auditor@co.ferry.wa.us>; mbeaton@co.franklin.wa.us <mbeaton@co.franklin.wa.us>; mlueck@co.garfield.wa.us <mlueck@co.garfield.wa.us>; mjaderlund@grantcountywa.gov <mjaderlund@grantcountywa.gov>; jmaclean@co.grays-harbor.wa.us <jmaclean@co.grays-harbor.wa.us>; s.crider@islandcountywa.gov <s.crider@islandcountywa.gov>; racarroll@co.jefferson.wa.us <racarroll@co.jefferson.wa.us>; Wise, Julie (King County) <Julie.Wise@kingcounty.gov>; pandrews@co.kitsap.wa.us <pandrews@co.kitsap.wa.us>; jerry.pettit@co.kittitas.wa.us <jerry.pettit@co.kittitas.wa.us>; brendas@klickitatcounty.org <brendas@klickitatcounty.org>; larry.grove@lewiscountywa.gov <larry.grove@lewiscountywa.gov>; rluiten@co.lincoln.wa.us <rluiten@co.lincoln.wa.us>; skf@masoncountywa.gov <skf@masoncountywa.gov>; chall@co.okanogan.wa.us <chall@co.okanogan.wa.us>; jkidd@co.pacific.wa.us <jkidd@co.pacific.wa.us>; mnichols@pendoreille.org <mnichols@pendoreille.org>; julie.anderson@co.pierce.wa.us <julie.anderson@co.pierce.wa.us>; mileneh@sanjuanco.com <mileneh@sanjuanco.com>; sandyp@co.skagit.wa.us <sandyp@co.skagit.wa.us>; rwaymire@co.skamania.wa.us <rwaymire@co.skamania.wa.us>; Garth.Fell@snoco.org <Garth.Fell@snoco.org>; Dalton, Vicky (SpokaneCounty) <VDalton@spokanecounty.org>; llarsen@stevenscountygov.wa <llarsen@stevenscountygov.wa>; hallm@co.thurston.wa.us <hallm@co.thurston.wa.us>; bergsengn@co.wahkiakum.wa.us <bergsengn@co.wahkiakum.wa.us>; kmmartin@co.walla-walla.wa.us <kmmartin@co.walla-walla.wa.us>; Dbradric@co.whatcom.wa.us <Dbradric@co.whatcom.wa.us>; auditor@co.whitman.wa.us <auditor@co.whitman.wa.us>; Charles.Ross@co.yakima.wa.us <Charles.Ross@co.yakima.wa.us>; SRCMEMBERS@leg.wa.gov <SRCMEMBERS@leg.wa.gov>; SDCMEMBERS@leg.wa.gov <SDCMEMBERS@leg.wa.gov>; HRCMEMBERS@leg.wa.gov <HRCMEMBERS@leg.wa.gov>; HDCMEMBERS@leg.wa.gov <HDCMEMBERS@leg.wa.gov>
Sent: August 20, 2021 3:59 PM (UTC-04:00)
Attached: Letter to Sec. Wyman and 39 WA County Auditors.pdf

Dear Representative Kraft,

Thank you for your letter. The Office of the Secretary of State values maintaining a collaborative relationship with state lawmakers in protecting the integrity of Washington elections.

The Office of the Secretary of State's retention policy for election records, both digital and paper, is publicly available online at the following website: https://www.sos.wa.gov/_assets/archives/recordsmanagement/office-of-the-secretary-of-state-records-retention-schedule-v.1.2-(june-....pdf.

With respect to your request for information about "a forensic image of your election systems," the Legislature has not required—and the Office of the Secretary of State does not have—such a record. Instead, the Legislature and Secretary of State have adopted many other safeguards to ensure the integrity of Washington's elections.

This request is now closed.

Regards,

Records/Public Disclosure
Office of Secretary of State
PO Box 40224 | Olympia, WA 98504-0224
360-704-7834 Fax
publicrecords@sos.wa.gov
www.sos.wa.gov

WASHINGTON
Secretary of State
Operations Division

The refusal to comply with **Representative Vicki Kraft's** request for a forensic audit in 2021 exemplifies the systemic resistance to transparency embedded within **Washington's** election infrastructure. The fact that a sitting state legislator—acting within her oversight role and seeking a forensic imaging of election systems before any software or hardware upgrades—was denied underlines the institutional barriers that prioritize secrecy over accountability. The response from then-**Secretary of State Kim Wyman**, asserting that there was no legislative or administrative precedent for such an audit, is emblematic of the entrenched resistance to independent assessments, even when these are necessary to ensure election security and public trust.

This denial occurred before the enactment of **SB5459** and prior to the amendments to **WAC 434-335-260**, making it clear that the state's refusal to allow third-party audits was not a reactive measure but a deliberate, preemptive strategy to insulate election systems from scrutiny. The refusal to conduct a forensic audit also disregards federal mandates like **EO 13800**, which emphasize the importance of third-party assessments for critical infrastructure. By rejecting even a legislator's request for transparency, the state demonstrated an overt commitment to avoiding independent oversight.

The timing of this request is particularly significant. Coming on the heels of the 2020 election—a period marked by heightened public concern over election integrity—the refusal signals an unwillingness to engage with valid questions about election system security. Forensic audits, unlike risk-limiting audits, offer a comprehensive evaluation of hardware, software, and data integrity, making them a cornerstone of compliance with federal cybersecurity standards. The outright dismissal of such a request highlights the systemic avoidance of measures designed to verify and strengthen the security of election systems.

This institutional resistance, compounded by the later codification of opacity through legislative and administrative changes, reinforces a troubling pattern: **Washington State's** election officials are not only neglecting their duty to comply with federal cybersecurity mandates but are also actively obstructing efforts to ensure public accountability. This denial of a forensic audit, even when requested by a state legislator, underscores the deliberate and coordinated nature of these efforts to block transparency at every level. It further exemplifies the broader issues discussed throughout this report,

where the state prioritizes administrative control and secrecy over the fundamental principles of democratic governance and election integrity.

The denial of a forensic audit request by then-**Washington Secretary of State Kim Wyman** takes on even greater significance when viewed in light of her subsequent appointment as **Senior Election Security Advisor** at **CISA** in November 2021. This transition from a state official responsible for overseeing Washington's election systems to a federal role guiding national election security underscores the troubling overlap between state-level administrative resistance and federal election infrastructure policy.

As **Secretary of State, Wyman** was instrumental in shaping **Washington's** election policies, including the denial of a forensic audit requested by **Representative Vicki Kraft.** Her refusal not only disregarded valid concerns raised by a sitting legislator but also violated the principles outlined in **Executive Order 13800**, which mandates adherence to the **NIST Cybersecurity Framework** and independent verification of critical infrastructure systems. This refusal, predicated on the claim of lacking legislative or administrative precedent, reveals a pattern of insulating election systems from meaningful scrutiny under the guise of maintaining control and order.

Wyman's elevation to a federal advisory role at **CISA**, an agency heavily involved in influencing state election practices, further ties her actions in **Washington** to broader national policies. Her appointment signifies an endorsement of the same approach she employed at the state level—emphasizing risk-limiting audits and administrative control while sidelining calls for independent third-party verification. As **CISA's Senior Election Security Advisor**, **Wyman** now wields influence over national election infrastructure, raising questions about the alignment of her past practices with federal policy and the implications for election transparency across the country.

This career trajectory is emblematic of the deep integration between state and federal approaches to election security, where officials who champion restrictive practices are elevated to roles that shape broader policy. **Wyman's** tenure as **Secretary of State** and her refusal to engage in forensic auditing exemplify the systemic resistance to transparency discussed throughout this report. Her subsequent federal role highlights the challenges of addressing these issues at both the state and national levels, as the same individuals driving opacity and resistance at the state level are positioned to reinforce these practices on a larger scale.

The implications are clear: the denial of third-party audits and forensic evaluations is not an isolated phenomenon but part of a coordinated strategy that transcends state boundaries. **Wyman’s** actions in **Washington** and her subsequent appointment to **CISA** illustrate the entrenchment of policies that prioritize administrative control and secrecy over public accountability and compliance with federal mandates. This intersection of state and federal roles demands closer scrutiny to ensure that election security policies genuinely serve the interests of transparency, accountability, and the democratic process.

Kim Wyman's appointment as **CISA's Senior Election Security Advisor** in 2021 placed her at the helm of shaping national election security policy, despite her record in **Washington State** of resisting independent audits and disregarding federal mandates like **EO 13800**. Her transition to a federal role underscores the deep integration between state-level administrative decisions and federal advisory bodies, raising significant concerns about the consistency and enforcement of election security standards nationwide.

This integration is further evidenced by **CISA**-led initiatives like the 2019 ***"Tabletop the Vote"*** exercise, which brought together federal and state stakeholders under the pretext of enhancing election security. These exercises, ostensibly designed to simulate and prepare for potential vulnerabilities, reveal a troubling pattern: federal advisory efforts prioritizing centralized control and narrative-building while omitting critical federal mandates such as **EO 13800** and the **NIST Cybersecurity Framework**. The focus on coordination and response, rather than compliance and accountability, highlights the systemic failure to uphold the standards required of critical infrastructure like election systems.

Tabletop the Vote 2019 Exercise

The ***"Tabletop the Vote 2019"*** exercise, as detailed through the accompanying ***PowerPoint Presentation*** and ***Draft Scenario***, provides a comprehensive view of a federal initiative to address election vulnerabilities. Organized under the leadership of **CISA**, part of **DHS**, this event brought together federal agencies, state election officials, private-sector vendors, and **NGO**s to simulate and mitigate potential threats to election infrastructure. However, despite its collaborative appearance, the exercise reveals systemic failures to adhere to federal laws, such as **Executive Order 13800**, and exposes a deliberate avoidance of the **NIST Cybersecurity Framework (CSF).** These

documents, while intended to portray readiness, ultimately highlight a reactive rather than preventative approach to election security.

The ***PowerPoint Presentation*** offers a strategic overview of the exercise, emphasizing response coordination and the involvement of various stakeholders. The ***Draft Scenario***, on the other hand, delves into specific vulnerabilities simulated during the exercise, such as ransomware attacks, voter registration database anomalies, and phishing campaigns. These scenarios underscore the emphasis on collaboration between federal, state, and private entities. Yet, both documents consistently sidestep addressing the requirements of **EO 13800**, a mandate in effect since 2017 that specifically requires rigorous third-party audits and adherence to federal cybersecurity standards for all critical infrastructure, including election systems. The omission of these mandates is glaring and indicative of a systemic disregard for the legal framework meant to secure the nation's democratic processes.

The participants in the exercise reflect a wide array of entities, each with significant roles in election management and cybersecurity. Federal agencies such as **DHS, FBI, NSA**, and the **Election Assistance Commission** were central to the exercise, providing guidance and coordinating responses. State-level officials, including **secretaries of state, election directors,** and **county auditors**, represented those directly responsible for administering elections. The private sector contributed through vendors like **Dominion Voting Systems, ES&S, Hart InterCivic, BlueCrest,** and **Runbeck**, whose proprietary systems and third-party dependencies are integral to election operations. Cybersecurity firms like **FireEye** and **CrowdStrike** were present, ostensibly to offer expertise in addressing digital threats, alongside **Microsoft**, which played a significant role through its **ElectionGuard** initiative and **Azure** cloud infrastructure. Non-governmental organizations such as **NASS, NASED**, and the **Center for Internet Security (via EI-ISAC)** acted as intermediaries, promoting information sharing between federal and state entities.

The **Department of Defense (DoD)**, through the **National Guard Bureau,** also participated, represented by **LTC Patrick Lewis and Dan Stafford.** Their involvement underscores the recognition of election systems as critical infrastructure tied to national security. However, the limited role of the **DoD** in this exercise raises concerns about the marginalization of military expertise in addressing cybersecurity threats. As representatives of an agency tasked with protecting critical infrastructure, they had both the authority and responsibility to identify and escalate the systemic failures evident in

this exercise. Their failure to ensure adherence to **EO 13800** and **NIST CSF** is troubling, given the **DoD's** broader mandate under **Presidential Policy Directive 21 (PPD-21).**

Both documents consistently emphasize advisory and informational mechanisms rather than enforcement and compliance. **CISA** and **EI-ISAC** are positioned as central coordinators, yet their roles are limited to advising and facilitating communication. This reliance on advisory entities bypasses the enforcement measures necessary to ensure election systems meet federal security standards. The focus on collaboration and response, while valuable, creates a facade of preparedness that masks the systemic failures to address root vulnerabilities. The scenarios outlined in the ***Draft Scenario*** document reveal long-standing issues such as outdated software, exploitable configurations, and insufficient training among election officials—problems that remain unaddressed due to the lack of independent third-party assessments.

The involvement of private vendors, including **Dominion Voting Systems, ES&S, Hart InterCivic, BlueCrest,** and **Runbeck,** further illustrates the deficiencies of this exercise. These vendors, responsible for the hardware and software underpinning election systems, were not scrutinized for their dependencies on third-party software or the vulnerabilities inherent in their proprietary systems. Similarly, **Microsoft's** involvement through **ElectionGuard** and **Azure** introduces risks associated with centralized data storage, yet these risks were not critically assessed. The absence of rigorous evaluation for these vendors directly contravenes **EO 13800's** mandate for independent compliance verification.

The documents also fail to address the risks introduced by cloud-based technologies and centralized data storage. While **Microsoft's Azure** was presented as a scalable and secure solution, its use poses significant cybersecurity challenges, particularly in light of the persistent vulnerabilities highlighted in the ***Election Infrastructure Cyber Risk Summary.*** These vulnerabilities, including exploitable services and delayed patching, often persisted for over 400 days—clear evidence of systemic neglect that contradicts **EO 13800's** emphasis on rapid risk mitigation.

The absence of **EO 13800** and the **NIST CSF** from these documents cannot be dismissed as a procedural oversight. It reflects a deliberate evasion of federal law and a broader resistance to independent oversight. These exercises, framed as collaborative efforts, ultimately serve as evidence of entrenched negligence among all participants.

The federal agencies, state officials, private vendors, and **NGO**s involved in this exercise cannot claim ignorance of these vulnerabilities or their legal obligations under federal mandates. Their collective failure to enforce or comply with these laws undermines the security of election systems and erodes public trust in the democratic process.

In conclusion, the ***"Tabletop the Vote 2019"*** exercise, as documented in the PowerPoint Presentation and Draft Scenario, exemplifies systemic failures in election security management. The reliance on advisory bodies, the exclusion of federal mandates, and the lack of vendor accountability reveal a reactive system that prioritizes optics over substance. The limited role of the **DoD** further underscores the lack of integration and accountability in addressing election vulnerabilities. These documents collectively expose a system designed to protect its own narrative rather than uphold the integrity of the electoral process, leaving critical infrastructure vulnerable and public trust eroded.

Tabletop the Vote 2019 MPM 2019_v00.pptx.pdf

https://docdro.id/Qi4gLv7

Tabletop The Vote 2019 Draft Scenario 20190409_v03.docx

https://docdro.id/CU1h5hd

TLP:AMBER Election Infrastructure Cyber Risk Summary

The **TLP:AMBER Election Infrastructure Cyber Risk Summary** provides a sobering insight into the vulnerabilities persisting within the U.S. election infrastructure, as well as the limited efficacy of existing measures to address them. Presented under the Traffic Light Protocol (TLP) classification system, the document is intended for controlled dissemination among stakeholders involved in election security. However, its findings reveal a glaring disconnect between the federal mandates designed to protect critical infrastructure—such as **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)**—and the actual state of election systems across the country.

The document outlines a range of vulnerabilities affecting election infrastructure, categorized primarily under digital threats, such as phishing campaigns, ransomware attacks, and unpatched software, as well as physical security concerns. Despite its detailed enumeration of risks, the summary lacks any substantive acknowledgment of federal cybersecurity requirements. Nowhere does it reference the mandates of **EO 13800**, which has been in place since 2017 to ensure robust protections for critical infrastructure sectors, including elections. This omission is not merely a procedural oversight but a systemic failure to prioritize compliance with federal law.

One of the most striking revelations in the document is the persistence of exploitable vulnerabilities. In some cases, risks were left unaddressed for over 400 days, despite being identified. This prolonged exposure contravenes the principles of **EO 13800**, which emphasize the immediate mitigation of risks. The failure to remediate known vulnerabilities not only undermines the security of election systems but also raises serious questions about the accountability of the entities responsible for managing these systems. It is evident that the reliance on vendor self-assessments and internal reporting mechanisms has led to a culture of complacency rather than proactive security.

The document highlights phishing as one of the most prevalent attack vectors targeting election officials. While it describes ongoing efforts to educate officials on recognizing and mitigating phishing attempts, this reactive approach underscores the systemic inadequacies in securing the underlying infrastructure. Rather than addressing the root causes of these vulnerabilities—such as outdated systems, insufficient access controls, and lack of adherence to cybersecurity best practices—the emphasis remains on incident response. This approach fails to align with the preventative measures required under the **NIST CSF**, which prioritizes risk management and resilience.

Another critical area of concern is the document’s discussion of ransomware attacks. While the summary outlines the potential impact of ransomware on voter registration databases and election reporting systems, it provides little guidance on how to prevent such attacks from occurring. The focus on responding to incidents after they occur reveals a reactive security posture that is wholly inadequate for protecting critical infrastructure. Moreover, the absence of independent third-party audits—a key requirement under **EO 13800**—means that vulnerabilities in these systems remain unaddressed and unverified by impartial assessors.

The document also discusses the use of cloud-based technologies in election systems, including centralized storage solutions. While it acknowledges the benefits of scalability and accessibility, it fails to address the significant risks posed by these technologies. Centralized systems introduce single points of failure, which are particularly vulnerable to cyberattacks. The summary's lack of critical analysis in this area highlights a broader reluctance to confront the inherent risks associated with modern technological dependencies.

One of the more troubling aspects of the document is its reliance on advisory mechanisms such as the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** and the **Cybersecurity and Infrastructure Security Agency (CISA)**. While these entities play essential roles in coordinating information sharing and incident response, their advisory nature does not compel compliance with federal standards. The reliance on voluntary participation and self-reporting undermines the accountability necessary to secure critical infrastructure effectively. Furthermore, the document's emphasis on information sharing over enforcement reflects a systemic aversion to the robust oversight mandated by federal law.

The absence of any discussion of vendor accountability is another critical oversight. Vendors such as **Dominion Voting Systems, ES&S,** and **Hart InterCivic,** which provide the hardware and software underpinning election systems, are central to the infrastructure's security. Yet, the document fails to scrutinize their practices or the vulnerabilities inherent in their proprietary systems. This omission is particularly concerning given the well-documented risks associated with third-party dependencies and outdated software components in these systems. By avoiding these discussions, the document perpetuates a reliance on vendor self-assessments that lack the rigor required to identify and mitigate vulnerabilities effectively.

The **TLP:AMBER** classification itself is worth scrutinizing. While the restricted dissemination of the document may be intended to protect sensitive information, it also serves to shield these systemic failures from public scrutiny. This lack of transparency undermines public trust in the election process and prevents the kind of accountability that is necessary to drive meaningful reform. The document's controlled distribution effectively insulates the entities responsible for these failures from external oversight, further compounding the issues it seeks to address.

In conclusion, the **TLP:AMBER Election Infrastructure Cyber Risk Summary** reveals more about what it omits than what it includes. Its failure to reference **EO 13800** and the **NIST CSF**, combined with its reliance on advisory mechanisms and vendor self-assessments, reflects a systemic reluctance to confront the underlying vulnerabilities in election infrastructure. The document highlights a reactive security posture that prioritizes incident response over prevention and accountability. By failing to enforce the robust protections mandated by federal law, the entities responsible for election security have left critical infrastructure exposed to persistent threats, undermining both the security of elections and public trust in democratic processes.

TLP_AMBER_Election_Infrastructure_Cyber_Risk_Summary.pdf

https://docdro.id/5B2vcsx

TLP:AMBER Election Infrastructure Cyber Risk Summary Fact Sheet

The **TLP:AMBER Election Infrastructure Cyber Risk Summary Fact Sheet** presents a detailed snapshot of systemic vulnerabilities within the U.S. election infrastructure, emphasizing persistent risks and outlining mitigation strategies. While the fact sheet appears to provide actionable insights, it ultimately highlights a pattern of inaction, reliance on advisory mechanisms, and an ongoing failure to adhere to federal mandates such as **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF)**. These systemic deficiencies underscore the broader failures of election security management in addressing both technological and procedural vulnerabilities.

The document reveals that between October 2020 and September 2021, significant risks persisted across the ***Election Infrastructure (EI) Subsector***. Notably, a median of 415 days passed before known exploited vulnerabilities were remediated, exposing critical systems to active threats for prolonged periods. This timeline starkly contrasts with the requirements of **EO 13800**, which mandates the rapid mitigation of risks in critical infrastructure. This inaction reflects a deep-seated culture of complacency and reliance on vendor self-assessments rather than the independent audits required to ensure transparency and accountability.

One of the most glaring insights is the continued operation of risky, internet-accessible services such as **NetBIOS, Telnet, SMB,** and **RDP**. These services, long recognized as exploitable entry points, remain prevalent across the sector. The document's recommendations to disable such services are framed as best practices rather than enforceable requirements, highlighting the advisory nature of the cybersecurity protocols in place. This leniency perpetuates systemic vulnerabilities, allowing attackers to exploit these weak points for initial access and lateral movement within networks.

The fact sheet also underscores phishing as a leading attack vector targeting election officials, with ongoing efforts to educate personnel on recognizing and mitigating such threats. However, this approach prioritizes incident response over the structural reforms needed to secure election systems. The reliance on phishing awareness training, while valuable, is insufficient when outdated systems and exploitable configurations remain unaddressed. This reactive stance exemplifies the broader inadequacies of the existing election security framework, which fails to align with the preventive measures outlined in the **NIST CSF**.

The issue of outdated software is another recurring theme in the fact sheet. Over 21.8% of scanned entities were found to be running unsupported operating systems, presenting a significant risk to election security. These systems, lacking vendor patches and updates, serve as attractive targets for attackers. This revelation is particularly troubling in light of **EO 13800's** mandate for robust cybersecurity protections, which clearly requires the timely replacement of unsupported technology. The persistence of these outdated systems signals a failure to enforce even basic cybersecurity hygiene.

The document also addresses the role of cloud-based solutions in election systems, emphasizing their scalability and accessibility. However, it fails to critically assess the risks introduced by centralized data storage. Cloud-based systems, particularly those relying on **Microsoft Azure** and **ElectionGuard**, present single points of failure that could compromise the integrity of election data. The absence of detailed risk assessments in this area reflects a broader reluctance to confront the challenges posed by modern technological dependencies.

Advisory mechanisms like the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** and **CISA's Albert Network Monitoring Service** are highlighted as essential resources for intelligence sharing and incident response. While these tools provide valuable insights, their advisory nature does not compel adherence to

federal cybersecurity standards. This reliance on voluntary compliance undermines the enforcement of robust security measures, further exacerbating the vulnerabilities outlined in the document.

The fact sheet's **TLP:AMBER** classification, intended to restrict its dissemination, raises additional concerns. While protecting sensitive information is a valid goal, this classification also shields systemic failures from public scrutiny. By limiting transparency, the document prevents the kind of accountability necessary to drive meaningful reform. This controlled dissemination reflects a broader strategy to insulate responsible entities from external oversight, perpetuating the very issues it seeks to address.

The omission of **EO 13800** and the **NIST CSF** from the fact sheet is particularly damning. These frameworks, explicitly designed to secure critical infrastructure, are entirely absent from the document's recommendations. This exclusion highlights a deliberate evasion of federal law and a broader reluctance to enforce the rigorous standards needed to secure election systems. By avoiding these mandates, the entities involved in election security prioritize administrative convenience over genuine accountability.

In its attempt to provide actionable insights, the ***TLP:AMBER Election Infrastructure Cyber Risk Summary Fact Sheet*** instead exposes the systemic flaws in the federal and state approaches to election security. The persistent vulnerabilities, reliance on advisory mechanisms, and absence of independent audits reveal a reactive posture that undermines the integrity of critical infrastructure. These failures, coupled with the controlled dissemination of findings, reflect a concerted effort to shield systemic negligence from public accountability. Without adherence to **EO 13800** and the **NIST CSF**, election systems remain vulnerable to exploitation, eroding public trust in the democratic process.

This document, like the broader election security framework it represents, highlights the urgent need for reform. Its findings serve as a reminder that without proactive enforcement of federal mandates, the security and transparency of elections will continue to be compromised.

TLP_AMBER Election Infrastructure Cyber Risk Summary Fact Sheet.pdf

https://docdro.id/a1vSoGO

Protect2020 Strategic Plan

The **"Protect2020 Strategic Plan"** lays out **CISA's** roadmap for securing election infrastructure in the lead-up to the 2020 general election. Framed as a comprehensive strategy, the document emphasizes collaboration among federal, state, local, and private-sector stakeholders to mitigate risks and ensure election integrity. However, a closer analysis reveals troubling gaps in enforcement, accountability, and alignment with federal mandates such as **EO 13800** and the **NIST Cybersecurity Framework (NIST CSF)**. While the plan projects an image of preparedness and proactive engagement, it ultimately reflects a systemic failure to address foundational vulnerabilities in election systems.

The document positions **CISA** as the lead coordinator for election security, highlighting its efforts to build trust among election officials and stakeholders through its #Protect2020 initiative. The strategy emphasizes three pillars: ***Protect, Prepare, and Promote Confidence***. These pillars ostensibly aim to safeguard election infrastructure, enhance preparedness through exercises and training, and foster public trust in the electoral process. While these goals are commendable, the plan's execution reveals a significant reliance on voluntary compliance, advisory mechanisms, and centralized control, rather than enforcing the robust standards mandated by federal law.

Central to the strategy is **CISA's** reliance on the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** as the primary conduit for intelligence sharing. While **EI-ISAC** plays an essential role in disseminating threat information, its advisory nature limits its effectiveness in enforcing compliance. The plan fails to incorporate the independent third-party audits and rigorous testing required under **EO 13800**, undermining the transparency and accountability necessary to secure critical infrastructure. This omission reflects a broader trend in **CISA's** approach: prioritizing collaboration and advisory roles over the enforcement of federal cybersecurity standards.

The **Protect pillar** emphasizes identifying and mitigating risks to election infrastructure. However, the measures outlined in the document focus on surface-level vulnerabilities, such as phishing attempts and ransomware, without addressing the root causes of these threats. The strategy's reliance on **Albert Network Monitoring sensors**, provided through **EI-ISAC**, highlights the document's dependence on proprietary monitoring tools. These tools, while useful for detecting anomalies, do not replace the need for

independent audits or comprehensive compliance testing. Moreover, the reliance on **Albert sensors** perpetuates a centralized model of oversight that conflicts with the decentralized nature of U.S. elections, further complicating accountability.

Under the **Prepare pillar**, the plan outlines initiatives such as tabletop exercises and training programs for election officials. These efforts, while valuable, often emphasize reactive responses to incidents rather than proactive measures to prevent vulnerabilities. The absence of **EO 13800** and **NIST CSF** compliance in these exercises further undermines their credibility. Without incorporating federal mandates into these scenarios, the exercises risk becoming performative rather than substantive, focusing on response coordination at the expense of addressing systemic flaws.

The **Promote Confidence pillar** aims to counter disinformation and bolster public trust in elections. However, this focus on narrative management diverts attention from the more pressing issue of ensuring the security and transparency of election systems. By prioritizing public perception over structural reforms, the strategy risks creating a false sense of security that undermines genuine accountability.

A particularly troubling aspect of the document is its lack of scrutiny toward vendors and third-party software dependencies. Vendors such as **Dominion Voting Systems, ES&S,** and **Hart InterCivic** are integral to the election infrastructure, yet the plan does not address the risks posed by their proprietary systems. The absence of independent audits for these vendors directly contradicts **EO 13800's** requirements, leaving significant vulnerabilities unexamined. Similarly, the plan's limited focus on cloud-based technologies, such as **Microsoft Azure**, reflects a reluctance to confront the inherent risks of centralized data storage and processing.

The plan also highlights partnerships with state and local officials as a cornerstone of its strategy. However, these partnerships are framed more as advisory relationships than enforceable agreements. This reliance on voluntary compliance allows state and local entities to bypass federal standards, further eroding the effectiveness of the strategy. The lack of mandatory adherence to **EO 13800** and **NIST CSF** across all jurisdictions creates a patchwork of compliance that leaves critical infrastructure vulnerable to exploitation.

The document's failure to incorporate **EO 13800** and **NIST CSF** into its framework is not merely an oversight but a systemic issue. By avoiding these mandates, **CISA** and its partners have sidestepped the independent oversight and rigorous standards necessary to

secure election systems. This deliberate evasion reflects a broader reluctance to enforce accountability, perpetuating the vulnerabilities that the strategy claims to address.

The **"Protect2020 Strategic Plan"** illustrates the systemic flaws in the federal approach to election security. While it emphasizes collaboration, preparation, and public confidence, its reliance on advisory mechanisms and voluntary compliance undermines its effectiveness. The plan's failure to enforce **EO 13800** and **NIST CSF**, coupled with its reliance on vendor self-assessments and centralized oversight, exposes critical infrastructure to ongoing threats. By prioritizing optics over substance, the strategy ultimately compromises both the security of elections and public trust in the democratic process.

Protect2020 Strategic Plan FINAL.pdf

https://docdro.id/zKWrRrO

Election Subsector Security Resources

The **"Election Subsector Security Resources"** document reflects an ongoing effort by **CISA** to provide election officials with tools and guidance to secure election infrastructure. However, despite its comprehensive appearance, the document falls short of addressing the fundamental issues that plague election security in the United States. By focusing on optional resources and advisory mechanisms, it sidesteps the enforcement of federal cybersecurity mandates, such as **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF)**, leaving critical vulnerabilities unaddressed.

At its core, the document is designed to offer election officials a range of resources categorized under physical security, cyber hygiene, incident response, and information sharing. These categories reflect a recognition of the diverse threats facing election infrastructure, from phishing and ransomware to physical tampering and insider threats. Yet, the reliance on voluntary compliance with these recommendations highlights a systemic flaw in the election security framework: the absence of mandatory enforcement mechanisms. The tools and services provided, while helpful, are framed as suggestions rather than requirements, allowing election officials and vendors to decide their level of engagement without accountability.

A recurring theme in the document is the emphasis on information sharing, particularly through entities like the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**. **EI-ISAC** is praised as a critical conduit for disseminating threat intelligence and coordinating responses to incidents. However, this reliance on information sharing does little to address the root causes of vulnerabilities. While sharing intelligence is valuable, it cannot replace the need for rigorous compliance testing and independent audits. The absence of these measures directly contravenes the mandates of **EO 13800**, which require comprehensive assessments to secure critical infrastructure.

The resources related to cyber hygiene, such as vulnerability scanning and phishing awareness programs, exemplify the document's reactive approach to security. These tools focus on identifying and responding to threats rather than preventing them. For example, the Cyber Hygiene Scanning service identifies vulnerabilities in internet-facing systems but does not mandate remediation. This permissive stance enables vulnerabilities to persist, undermining the integrity of election systems. Similarly, the emphasis on phishing awareness training, while useful, fails to address the structural weaknesses that make phishing attacks possible, such as outdated systems and insufficient access controls.

Another area of concern is the document's treatment of third-party software and vendor dependencies. Vendors like **Dominion Voting Systems, ES&S**, and **Hart InterCivic** are integral to election infrastructure, yet the document does not address the risks posed by their proprietary systems or third-party software components. This omission reflects a broader reluctance to scrutinize vendors, perpetuating a reliance on self-assessments rather than the independent verification required by federal mandates. The lack of vendor accountability is particularly troubling given the well-documented vulnerabilities associated with these systems, from exploitable software configurations to outdated hardware.

The focus on physical security resources further underscores the document's reactive posture. Measures such as physical access controls and insider threat mitigation are important but do not address the systemic issues in digital security. The reliance on these measures, alongside advisory mechanisms, creates a false sense of security that diverts attention from the need for comprehensive compliance with federal standards.

Perhaps the most glaring omission is the lack of reference to **EO 13800** and the **NIST CSF**. These frameworks are foundational to securing critical infrastructure, providing clear guidelines for risk management, incident response, and system resilience. The document's failure to incorporate these mandates reveals a deliberate evasion of accountability, allowing election systems to remain vulnerable under the guise of voluntary improvement. This omission is particularly concerning given the persistence of known vulnerabilities, some of which have gone unremediated for over a year, as highlighted in related **CISA** reports.

The **"Election Subsector Security Resources"** document highlights the systemic flaws in the federal approach to election security. By emphasizing voluntary resources and advisory mechanisms, it fails to enforce the rigorous standards necessary to secure critical infrastructure. The absence of **EO 13800** and **NIST CSF** from its framework, coupled with its reliance on vendor self-assessments and optional participation, reflects a broader reluctance to confront the systemic vulnerabilities that threaten election integrity. While the document aims to provide a roadmap for securing election systems, it ultimately perpetuates the reactive posture that has left these systems exposed to persistent threats. Without meaningful reform and adherence to federal mandates, the resources outlined in this document will remain insufficient to protect the democratic process.

security_resources_election_subsector_508.pdf

https://docdro.id/FMMPfdk

NVPF-Situational Awareness - Deck

The **"NVPF-Situational Awareness"** deck presents an overview of situational awareness strategies designed to address threats and vulnerabilities in election systems. Prepared for stakeholders involved in the electoral process, this presentation emphasizes the importance of real-time monitoring, coordination, and information sharing to safeguard elections. However, beneath its surface of proactive engagement, the document reveals significant shortcomings in its alignment with federal mandates and its ability to address the systemic vulnerabilities that persist in election infrastructure.

The deck underscores situational awareness as a cornerstone of election security, focusing on the need for election officials to monitor threats and respond quickly to

incidents. It highlights tools and strategies such as threat intelligence platforms, incident reporting mechanisms, and collaborative efforts among federal, state, and local entities. While these components are crucial, the presentation's focus on reactionary measures rather than proactive compliance testing reflects a broader failure to adhere to the mandates of **EO 13800** and the **NIST Cybersecurity Framework (NIST CSF).**

A central theme of the presentation is the reliance on information sharing through entities like the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** and its parent organization, the **Center for Internet Security (CIS)**. While these bodies play an important role in disseminating intelligence, their advisory nature does not compel election entities to address identified vulnerabilities. This reliance on voluntary participation allows critical weaknesses to persist unchecked, undermining the integrity of election systems.

The document also emphasizes the importance of incident reporting, encouraging election officials to report anomalies and breaches to federal agencies such as **CISA** and the **FBI**. While this guidance is valuable, it reflects a reactive approach that prioritizes response over prevention. The absence of mandatory compliance with **EO 13800** and **NIST CSF** requirements further exacerbates this issue. By failing to incorporate independent audits and rigorous testing into its framework, the presentation perpetuates a culture of complacency rather than accountability.

One of the key insights from the deck is its discussion of threat actors and attack vectors. It identifies foreign interference, insider threats, and cyberattacks such as phishing and ransomware as primary concerns. However, the strategies outlined to mitigate these risks focus on monitoring and response rather than addressing the root causes of vulnerabilities. For example, while the deck highlights the importance of securing voter registration databases, it does not address the systemic weaknesses in the software and hardware that underpin these systems. This omission reflects a reluctance to confront the proprietary and third-party dependencies that continue to compromise election security.

The deck's emphasis on real-time monitoring also raises questions about the role of centralized technologies in election processes. Tools like **Albert Network Monitoring sensors**, provided by **EI-ISAC**, are designed to detect anomalies in network traffic. While these tools are valuable, their reliance on centralized oversight introduces potential risks, such as single points of failure and overdependence on proprietary

technologies. Moreover, the absence of transparency in how these tools operate and their effectiveness in mitigating threats undermines public trust in their deployment.

Another critical area of concern is the presentation's lack of scrutiny toward vendors and their role in election security. Vendors such as **Dominion Voting Systems, ES&S,** and **Hart InterCivic** are integral to the election infrastructure, yet the document does not address the risks associated with their systems. This omission is particularly troubling given the well-documented vulnerabilities in proprietary election technology, from outdated software to exploitable hardware configurations. By failing to mandate third-party audits for these vendors, the strategies outlined in the deck fall short of ensuring the security and integrity of election systems.

The situational awareness strategies also fail to account for the broader requirements of **EO 13800** and **NIST CSF**. These mandates emphasize not only risk identification and incident response but also the proactive measures necessary to secure critical infrastructure. The deck's focus on information sharing and response coordination neglects the need for independent verification and compliance testing, which are essential for addressing systemic vulnerabilities.

In conclusion, the **"NVPF-Situational Awareness"** deck highlights the reactive posture that has come to define federal and state approaches to election security. While it emphasizes real-time monitoring and collaboration, it neglects the foundational requirements of **EO 13800** and **NIST CSF**, which prioritize prevention and accountability. The reliance on advisory mechanisms, the absence of vendor scrutiny, and the failure to enforce compliance standards reflect a systemic reluctance to confront the underlying vulnerabilities in election infrastructure. Without meaningful reform and adherence to federal mandates, the strategies outlined in this document will remain insufficient to secure the electoral process and restore public trust in democratic institutions.

NVPF-Situational Awareness - Deck.pdf - Google Drive.pdf

https://docdro.id/xGmubB0

Healthcare and Public Health (HPH) Government Coordinating Council (GCC)Charter

The **"HPH-GCC Charter (2016)"**, which establishes the governance framework for the **Healthcare and Public Health (HPH) Government Coordinating Council (GCC),** offers significant insights into the operational dynamics of federal oversight in critical infrastructure sectors. While its primary focus is on the healthcare and public health subsector, its principles and practices provide a lens through which to evaluate similar governance structures, such as those overseeing election infrastructure. The document underscores recurring issues, including the balance between advisory roles and enforcement authority, the integration of public-private partnerships, and the adherence to federal cybersecurity mandates.

The charter begins by outlining the mission and objectives of the **HPH-GCC**, emphasizing collaboration between federal, state, local, tribal, and territorial governments to protect critical infrastructure. This collaborative approach mirrors the structure of the Election Infrastructure Subsector, where entities like **CISA** and **EI-ISAC** play central roles in coordinating efforts. However, the reliance on collaboration over enforcement becomes a recurring theme that undermines the effectiveness of these councils. The advisory nature of the **HPH-GCC,** like its election infrastructure counterparts, limits its ability to compel compliance with federal mandates such as **EO 13800** and the **NIST Cybersecurity Framework (NIST CSF).**

One of the key principles highlighted in the charter is the reliance on public-private partnerships to enhance infrastructure resilience. While this approach facilitates the sharing of expertise and resources, it also introduces significant risks, particularly when private sector entities are not subject to the same accountability standards as their government counterparts. In the context of election infrastructure, this reliance has led to systemic vulnerabilities, as evidenced by the lack of independent audits for vendors like **Dominion Voting Systems** and **ES&S**. The absence of rigorous oversight in these partnerships compromises the integrity of critical infrastructure sectors, whether in healthcare or elections.

The charter also emphasizes information sharing as a core function of the **HPH-GCC**. This parallels the role of **EI-ISAC** in election security, where information sharing is prioritized over direct enforcement of security standards. While the sharing of threat intelligence is essential, it does not address the root causes of vulnerabilities. In the case

of election infrastructure, this approach has perpetuated a reactive security posture that prioritizes incident response over proactive measures like compliance testing and risk mitigation.

Another significant theme in the charter is the delineation of roles and responsibilities among federal, state, and local entities. The **HPH-GCC** explicitly acknowledges the sovereignty of state and local governments in managing critical infrastructure. However, it also underscores the federal government's role in providing guidance and resources. This dynamic creates a delicate balance that, in the context of election security, has often tipped in favor of state sovereignty at the expense of federal enforcement. The reluctance to mandate adherence to **EO 13800** and **NIST CSF** reflects this imbalance, allowing states to sidestep critical cybersecurity requirements under the guise of federalism.

The document's focus on voluntary participation further highlights the limitations of the **GCC** model. Membership in the council is not mandatory, and its recommendations are non-binding. This structure undermines the council's ability to enforce compliance with federal standards, leaving critical infrastructure sectors vulnerable to persistent threats. In the election infrastructure context, this voluntary framework has allowed systemic vulnerabilities to persist, as vendors and election officials are not compelled to implement robust security measures.

One area where the **HPH-GCC** Charter diverges from election infrastructure governance is its emphasis on sector-specific expertise. The healthcare and public health subsector benefits from a wealth of technical knowledge and established best practices, which are integrated into its governance framework. In contrast, election infrastructure governance has struggled to incorporate similar levels of expertise, particularly in the realm of cybersecurity. This gap has been exacerbated by the exclusion of **EO 13800** and **NIST CSF** from election security frameworks, which undermines the development of comprehensive risk management strategies.

The charter's commitment to fostering resilience is noteworthy but insufficient without enforceable standards. While resilience is a critical component of critical infrastructure security, it cannot replace the need for accountability and compliance. The failure to enforce **EO 13800** and **NIST CSF** in election infrastructure governance reflects a broader reluctance to impose the stringent measures necessary to secure critical systems.

In conclusion, the **HPH-GCC Charter (2016)** provides valuable insights into the governance challenges facing critical infrastructure sectors. Its reliance on advisory roles, voluntary participation, and public-private partnerships mirrors the systemic flaws in election infrastructure governance. By prioritizing collaboration over enforcement, these frameworks fail to address the root causes of vulnerabilities, leaving critical systems exposed to persistent threats. The lessons drawn from the **HPH-GCC Charter** underscore the urgent need for meaningful reform in election infrastructure governance, with a focus on enforcing federal mandates, enhancing accountability, and integrating technical expertise.

hph-gcc-charter-2016-508.pdf

https://docdro.id/YvbASP8

Healthcare and Public Health Sector Coordinating Council Charter

The **Healthcare and Public Health Sector Coordinating Council Charter** provides an organizational framework for coordinating efforts to protect one of the nation's most vital critical infrastructure sectors. Like other coordinating council charters, it emphasizes the importance of collaboration between public and private entities, aiming to build resilience and enhance security through shared responsibilities. However, the document also highlights systemic weaknesses that are not unique to healthcare but are mirrored across critical infrastructure sectors, including elections. These weaknesses—rooted in voluntary compliance, a lack of enforceable standards, and over-reliance on advisory mechanisms—pose significant risks to national security.

At its core, the charter prioritizes public-private partnerships as the cornerstone of its governance structure. This approach, while fostering collaboration, is inherently limited by its voluntary nature. Participation is not mandated, nor are the recommendations or best practices outlined in the charter enforceable. This permissive model creates gaps in accountability, where key stakeholders can evade responsibility for systemic vulnerabilities. Such a framework mirrors the dynamics seen in election infrastructure governance, where similar reliance on voluntary compliance undermines efforts to secure critical systems.

One of the central themes of the charter is information sharing, facilitated through mechanisms like the **Healthcare and Public Health Sector Information Sharing and Analysis Center (HPH-ISAC)**. While information sharing is undoubtedly valuable, it cannot replace the enforcement of rigorous security standards. The emphasis on intelligence dissemination assumes that stakeholders will act on shared information, but without mechanisms to compel action, critical vulnerabilities remain unresolved. This dynamic is strikingly similar to the shortcomings of the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**, where shared intelligence often fails to translate into actionable security improvements.

The document also highlights the role of private vendors and third-party service providers in supporting healthcare infrastructure. These entities, while integral to the sector's operations, introduce significant risks through proprietary technologies and insufficient transparency. The charter does not address the accountability of these vendors, perpetuating a reliance on self-assessments that lack the rigor needed to identify and mitigate vulnerabilities. In the context of election infrastructure, this same issue has allowed vendors like **Dominion Voting Systems** and **ES&S** to operate without meaningful oversight, exacerbating risks to system integrity.

One of the most glaring omissions in the charter is its failure to integrate federal mandates such as **Executive Order 13800** and the **NIST Cybersecurity Framework.** These mandates establish clear requirements for securing critical infrastructure, including independent third-party audits and compliance testing. By excluding these frameworks, the charter reflects a systemic reluctance to enforce the accountability necessary to secure critical systems. This omission is not unique to healthcare; it is a recurring theme across sector-specific governance documents, highlighting a broader pattern of neglect.

The reliance on advisory mechanisms rather than enforceable standards creates a reactive security posture that prioritizes incident response over prevention. While the charter outlines the importance of coordinated responses to emergencies, it does not address the root causes of vulnerabilities or the systemic changes needed to prevent breaches. This approach, though well-intentioned, fails to align with the proactive measures outlined in **EO 13800** and the **NIST CSF,** which emphasize risk management and resilience.

The absence of enforceable standards is particularly troubling given the interdependencies between critical infrastructure sectors. Healthcare and public health systems are deeply connected to other sectors, including emergency services and elections. Vulnerabilities in one sector can have cascading effects across others, amplifying risks to national security. For example, the increasing reliance on cloud-based technologies and centralized data systems introduces single points of failure that are attractive targets for cyberattacks. Yet, the charter does not critically address these risks, leaving systemic vulnerabilities unmitigated.

In the context of election security, the governance model outlined in the **HPH-SCC Charter** underscores the broader issues that plague critical infrastructure protection. Both sectors rely on complex networks of stakeholders, yet their governance frameworks lack the enforcement mechanisms needed to secure these systems effectively. The reliance on voluntary compliance and information sharing creates a facade of preparedness that belies the underlying weaknesses in their security postures.

The **Healthcare and Public Health Sector Coordinating Council Charter** exemplifies the challenges of balancing collaboration with accountability. Its emphasis on public-private partnerships and shared responsibility reflects a commendable effort to build resilience, but its permissive structure ultimately undermines its objectives. By failing to integrate federal mandates like **EO 13800** and the **NIST CSF**, the charter perpetuates a culture of voluntary action that leaves critical vulnerabilities unaddressed. This systemic reluctance to enforce accountability is a recurring theme across critical infrastructure governance, with implications that extend far beyond healthcare to include election systems and other vital sectors.

To secure critical infrastructure effectively, governance frameworks must move beyond voluntary participation and advisory mechanisms. They must incorporate enforceable standards that hold stakeholders accountable for systemic vulnerabilities. Without such reforms, sectors like healthcare and elections will remain exposed to persistent threats, compromising both their operational integrity and public trust. The **HPH-SCC Charter**, much like its counterparts in other sectors, serves as a stark reminder of the need for meaningful change in how we protect the nation’s most vital systems.

HPH-SCC Charter - dated-508_0.pdf

https://docdro.id/SRCic71

Healthcare and Public Health
Sector Council Charters Membership

The **"Healthcare and Public Health Sector Council Charters Membership"** document outlines the roles, responsibilities, and collaborative framework for the **Healthcare and Public Health (HPH) Sector Councils.** As part of the broader effort to safeguard critical infrastructure, this document provides insight into the governance and operational dynamics of one of the nation's most vital sectors. While its intent is to foster resilience and enhance security through public-private collaboration, the document reveals recurring systemic weaknesses that compromise the effectiveness of critical infrastructure governance. These issues resonate with similar failures in election infrastructure and other critical sectors.

The document emphasizes the dual council structure of the **HPH Sector: the Government Coordinating Council (GCC)** and the **Sector Coordinating Council (SCC)**. This structure is designed to ensure collaboration between public entities—such as federal, state, tribal, and local governments—and private stakeholders, including industry representatives and third-party service providers. While this model seeks to leverage diverse expertise, it is inherently limited by its reliance on voluntary participation and non-binding recommendations. The absence of enforceable requirements undermines the councils' ability to address vulnerabilities comprehensively.

A key feature of the document is its focus on information sharing as a primary tool for mitigating risks. Mechanisms like the **Healthcare and Public Health Sector Information Sharing and Analysis Center (HPH-ISAC)** play a central role in facilitating the exchange of intelligence among stakeholders. However, this approach falls short in addressing systemic vulnerabilities. Information sharing, while valuable, is not a substitute for mandatory compliance with federal cybersecurity standards. The reliance on voluntary action leaves critical gaps in accountability, allowing risks to persist unmitigated.

Vendor dependencies represent a significant area of concern. The **HPH Sector** relies heavily on private vendors for hardware, software, and services, many of which introduce vulnerabilities into the system. These dependencies mirror those in election infrastructure, where vendors like **Dominion Voting Systems** and **ES&S** have operated with minimal oversight. The document does not address the risks posed by these

dependencies or provide mechanisms for independent audits and compliance testing. This omission perpetuates a reliance on self-assessments that lack the rigor needed to identify and mitigate vulnerabilities effectively.

The document also highlights the interdependencies between the **HPH Sector** and other critical infrastructure sectors, such as communications, emergency services, and elections. These connections amplify the risks associated with systemic vulnerabilities. A compromise in one sector can have cascading effects across others, underscoring the need for robust, enforceable standards. Despite this, the councils' governance model prioritizes voluntary collaboration over mandatory compliance, leaving the sector exposed to persistent threats.

One of the most troubling aspects of the document is its failure to integrate federal mandates like **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF).** These frameworks provide clear, enforceable standards for securing critical infrastructure, yet the document relies on advisory mechanisms that lack the authority to compel compliance. This omission reflects a systemic reluctance to enforce accountability, perpetuating a reactive security posture that prioritizes incident response over prevention.

The permissive structure of the councils is particularly concerning given the high stakes associated with the **HPH Sector**. As the sector responsible for safeguarding public health, its vulnerabilities have direct implications for national security and public trust. The reliance on voluntary participation and self-regulation creates a facade of preparedness that belies the underlying weaknesses in its governance framework.

The **"Healthcare and Public Health Sector Council Charters Membership"** document exemplifies the systemic deficiencies that undermine critical infrastructure governance. Its reliance on voluntary collaboration, lack of enforceable standards, and omission of federal mandates like **EO 13800** and the **NIST CSF** reveal a broader reluctance to confront the structural issues compromising national security. For the **HPH Sector** to fulfill its critical role effectively, its governance framework must evolve to prioritize enforceable standards, independent oversight, and accountability. Without these changes, the vulnerabilities highlighted in this document will continue to jeopardize public health, national security, and public trust.

Healthcare and Public Health Sector. Council Charters Membership . CISA.pdf

https://docdro.id/H8SRe5o

Guide to Securing Remote Access Software

The **"Guide to Securing Remote Access Software"** offers a glimpse into federal efforts to address the risks associated with remote access technologies. While the guide is framed as a practical resource for organizations managing critical infrastructure, its contents reveal a significant disconnect between advisory recommendations and enforceable measures. This disparity is particularly troubling in the context of election infrastructure, where the implications of unsecured remote access extend beyond operational concerns to the very foundation of democratic processes.

At its core, the guide acknowledges the inherent vulnerabilities in remote access software. These technologies, essential for managing modern infrastructure, open pathways for unauthorized access, malware deployment, and lateral movement across networks. Yet, the guide's approach to mitigating these risks relies heavily on best practices and voluntary implementation. This advisory posture sidesteps the foundational mandates of **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF)**, both of which demand rigorous, enforceable standards for securing critical infrastructure.

The omission of **EO 13800** is glaring, particularly given its explicit requirement for independent assessments and third-party audits. The reliance on organizations to self-assess their compliance with vague guidelines creates an environment where vulnerabilities are allowed to persist unchecked. This permissive stance is evident throughout the guide, which offers suggestions for securing remote access tools but refrains from imposing the accountability necessary to ensure compliance.

One of the guide's primary focuses is on limiting third-party access to remote systems, a recommendation that reflects a clear understanding of the risks posed by vendor dependencies. However, it stops short of addressing the systemic vulnerabilities introduced by the vendors themselves. Companies like **Dominion Voting Systems, ES&S**, and **Hart InterCivic**, which play critical roles in election infrastructure, often integrate remote access capabilities into their systems. These features, while convenient, create significant attack surfaces that are poorly managed under the current framework. The guide's failure to mandate third-party audits for these vendors perpetuates a reliance

on proprietary assessments that lack the transparency and rigor needed to identify and address weaknesses.

The emphasis on access controls, such as multi-factor authentication and network segmentation, provides practical advice but reflects a reactive rather than proactive approach. These measures, while effective at mitigating immediate threats, do not address the root causes of vulnerabilities in remote access tools. For example, outdated or improperly maintained software remains a common issue, yet the guide does not include mechanisms for enforcing timely updates or patches. The absence of proactive compliance measures undermines the efficacy of these recommendations.

One of the more concerning aspects of the guide is its focus on incident response planning. While having protocols in place to detect and respond to breaches is essential, this emphasis underscores a broader pattern of prioritizing damage control over prevention. This reactive posture is emblematic of a systemic failure to address vulnerabilities before they can be exploited. In the context of election infrastructure, this approach is particularly troubling, as the consequences of a breach extend far beyond operational disruptions to include loss of public trust and potential manipulation of electoral outcomes.

The guide also touches on the use of centralized technologies, including cloud-based solutions, for managing remote access. While it highlights the scalability and convenience of these systems, it glosses over the significant risks they introduce. Centralized systems, by their nature, create single points of failure that are particularly attractive to cyber attackers. The guide’s lack of critical analysis in this area reflects a broader reluctance to confront the vulnerabilities inherent in modern technological dependencies. In the election context, where cloud-based storage and processing are increasingly prevalent, this oversight is especially concerning.

Ultimately, the **Guide to Securing Remote Access Software** exemplifies the challenges of balancing convenience with security. While it provides valuable insights into mitigating immediate risks, its reliance on voluntary compliance and self-assessment undermines its potential effectiveness. By failing to integrate the robust standards outlined in **EO 13800** and the **NIST CSF**, the guide misses an opportunity to enforce meaningful reforms that could secure remote access tools across critical infrastructure sectors.

In the broader context of election security, this guide highlights systemic vulnerabilities that remain unaddressed. Remote access tools, while indispensable, represent significant points of entry for potential exploitation. Without enforceable standards and independent oversight, the risks associated with these technologies will continue to compromise both the security of election systems and public confidence in democratic processes. By prioritizing advisory recommendations over mandatory compliance, the guide reflects a broader reluctance to confront the structural issues that undermine election infrastructure security.

GuidetoSecuringRemoteAccessSoftware_cleanFinal_508c.pdf

https://docdro.id/EKThFJW

Emergency Services Sector Coordinating Council Charter

The **Emergency Services Sector Coordinating Council Charter** presents itself as a blueprint for protecting one of the nation's most critical infrastructure sectors. It leans heavily on the idea of public-private partnerships and voluntary collaboration to address threats. However, upon closer scrutiny, it becomes apparent that the charter, while well-meaning, is emblematic of the broader systemic issues that plague critical infrastructure governance in the United States. This approach, centered on optional compliance and advisory mechanisms, leaves foundational vulnerabilities unaddressed—an oversight with profound implications for emergency services and other critical systems like election infrastructure.

At its core, the charter emphasizes the importance of cooperation between government agencies and private stakeholders, presenting a shared responsibility model. This structure has clear potential: pooling resources and expertise to mitigate risks. Yet, without enforceable requirements, the council's efforts rely entirely on the goodwill and discretionary action of its participants. This voluntary nature undermines the efficacy of any recommendations or strategies that emerge. In practice, it allows systemic weaknesses to persist unchecked, perpetuating an environment where accountability is fragmented and security efforts are inconsistent.

This dynamic parallels the challenges faced in election security. Much like the **Emergency Services Sector**, election systems rely on intricate networks of federal, state, and private entities. In both cases, reliance on third-party vendors introduces

significant vulnerabilities. The charter, however, makes no meaningful provisions for addressing the risks associated with these dependencies. In the election context, vendors like **Dominion Voting Systems** and **ES&S** operate with proprietary technologies that remain largely unexamined by independent assessors. Similarly, private vendors supporting emergency services are left to self-regulate, creating a systemic blind spot where vulnerabilities flourish unchecked.

The emphasis on information sharing within the charter reflects an inherent belief that intelligence alone can drive action. Facilitated through platforms like the **National Infrastructure Coordinating Center**, this approach prioritizes situational awareness and the dissemination of threat intelligence. However, intelligence without enforcement mechanisms accomplishes little. This model assumes that all stakeholders will act on shared information, but without mandatory compliance, such action often remains theoretical. The result is a system that can identify risks but lacks the tools to compel mitigation.

In election infrastructure, this reliance on voluntary action has proven inadequate. Mechanisms like the **Election Infrastructure Information Sharing and Analysis Center** have enhanced information sharing but failed to address the root causes of vulnerabilities. Without enforceable standards, the risks persist, creating the illusion of progress without substantive improvement. The **Emergency Services Sector** faces a similar predicament, where the potential of shared intelligence is undermined by the lack of enforceable actions.

One of the most troubling aspects of the charter is its failure to align with existing federal mandates. Critical infrastructure sectors, including emergency services, are subject to the requirements of **Executive Order 13800** and the **NIST Cybersecurity Framework**. These mandates provide clear directives for securing systems against cyber threats, including the necessity for independent audits and rigorous compliance testing. Yet, the charter makes no mention of these frameworks. This omission reflects a broader reluctance across critical infrastructure governance to enforce federal standards, perpetuating a culture of voluntary participation that prioritizes convenience over accountability.

This reluctance to enforce standards has broader implications for national security. Emergency services and election systems are both integral to public trust and national resilience. The vulnerabilities in one sector can ripple across others, exacerbating risks

in interconnected systems. For instance, both sectors rely on outdated technologies and centralized data systems that introduce significant risks. Yet, governance frameworks like the **Emergency Services Sector Coordinating Council Charter** sidestep these issues, focusing instead on cooperative rhetoric that lacks the teeth to drive meaningful change.

In practice, this permissive approach fosters a systemic failure to address vulnerabilities comprehensively. The reliance on voluntary compliance allows entities to opt out of necessary security measures, perpetuating weaknesses that threaten the integrity and resilience of critical systems. The absence of rigorous enforcement mechanisms also enables private vendors to operate without accountability, shielding their proprietary technologies from scrutiny. This lack of transparency and oversight undermines the resilience these governance structures claim to protect.

The **Emergency Services Sector Coordinating Council Charter** reflects the same systemic deficiencies that undermine election security governance. Its reliance on voluntary collaboration and advisory mechanisms creates a facade of preparedness that belies its fundamental weaknesses. By failing to integrate enforceable standards like **EO 13800** and the **NIST Cybersecurity Framework**, it perpetuates a reactive security posture that prioritizes optics over substance. For both emergency services and election systems, this approach leaves critical vulnerabilities unaddressed, jeopardizing public trust and national security. If these sectors are to be truly resilient, their governance structures must move beyond voluntary cooperation to enforce the accountability necessary for meaningful reform.

emergency-services-sector-coordinating-council-charter-032018-508.pdf

https://docdro.id/lvDZ5rN

Emergency Services Government Coordinating Council Charter (2020)

The **Emergency Services Government Coordinating Council Charter (2020)** serves as a foundational document for structuring the collaborative efforts of federal, state, tribal, and local entities tasked with safeguarding the emergency services sector. While the charter's stated goals include enhancing resilience, security, and operational

readiness, its reliance on voluntary participation and its lack of enforceable standards reveal deep-seated vulnerabilities. These structural flaws mirror those found in other critical infrastructure sectors, such as election systems, further emphasizing the systemic nature of these governance issues.

The charter defines the roles and responsibilities of participating entities, prioritizing collaboration, information sharing, and public-private partnerships. It establishes a framework where government entities work alongside private stakeholders to identify and mitigate risks. However, the document stops short of mandating compliance with federal cybersecurity standards, such as those outlined in **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)**. This omission significantly undermines the charter’s effectiveness, as it prioritizes cooperation over accountability, allowing vulnerabilities to persist across the sector.

One of the charter's central themes is the facilitation of information sharing through mechanisms like the **Homeland Security Information Network (HSIN).** While this approach aims to enhance situational awareness and foster coordinated responses to threats, it relies entirely on voluntary participation. There are no provisions to compel stakeholders to act on shared intelligence, leaving critical vulnerabilities unaddressed. This dynamic is emblematic of broader governance failures across critical infrastructure, where information sharing often substitutes for meaningful enforcement of security standards.

Vendor dependencies represent another critical oversight in the charter. The emergency services sector, like election systems, relies heavily on third-party technologies and service providers. These dependencies introduce significant risks, including exploitable vulnerabilities in proprietary systems, outdated software, and a lack of transparency in vendor operations. The charter does not address these risks or mandate independent audits or third-party compliance testing, perpetuating a reliance on vendor self-assessments that are insufficient for identifying and mitigating systemic vulnerabilities.

The charter’s permissive structure is particularly troubling given the emergency services sector's critical role in national security. Emergency services are inherently interconnected with other critical infrastructure sectors, including communications, healthcare, and elections. A compromise in this sector could have cascading effects, amplifying risks across the entire infrastructure ecosystem. Despite this, the charter

lacks the enforceable mechanisms necessary to ensure the sector's resilience, reflecting a broader reluctance to impose accountability in critical infrastructure governance.

The absence of federal mandates, such as **EO 13800** and the **NIST CSF**, is a glaring omission in the charter. Both of these frameworks provide clear, enforceable standards for securing critical infrastructure, yet the charter relies on advisory mechanisms that lack the authority to compel compliance. This failure to integrate federal cybersecurity mandates highlights a systemic neglect that undermines the resilience of not only the emergency services sector but also interconnected systems like elections.

The reliance on voluntary participation and self-regulation creates a reactive security posture that prioritizes incident response over prevention. While the charter emphasizes the importance of coordinated responses to emergencies, it does not address the systemic changes needed to prevent vulnerabilities from being exploited in the first place. This approach leaves the sector exposed to persistent threats, eroding public trust and compromising national security.

The **Emergency Services Government Coordinating Council Charter** reflects the broader challenges facing critical infrastructure governance. Its reliance on voluntary collaboration, permissive standards, and advisory mechanisms perpetuates systemic vulnerabilities that undermine the sector's resilience. By failing to integrate federal mandates like **EO 13800** and the **NIST CSF**, the charter misses an opportunity to enforce accountability and drive meaningful reforms. For emergency services and other critical infrastructure sectors to fulfill their roles effectively, their governance frameworks must evolve to prioritize enforceable standards and independent oversight. Without these changes, the systemic weaknesses highlighted in this charter will continue to jeopardize the nation’s security and public trust.

emergency-services-government-coordinating-council-charter-102020-508.pdf

https://docdro.id/bKJ5pqu

Communications Government Coordinating Council Charter (2020)

The **"Communications Government Coordinating Council Charter"** outlines the governance structure for managing risks and ensuring resilience in the communications

sector, a critical infrastructure that underpins nearly every other sector, including emergency services, healthcare, and elections. While this charter focuses on the communications sector, its framework shares notable similarities with other government coordinating councils, such as those for emergency services and public health. As with these other charters, it highlights systemic vulnerabilities rooted in voluntary compliance, lack of enforceable standards, and reliance on advisory mechanisms.

The charter emphasizes the importance of cross-sector collaboration and coordination among federal, state, local, tribal, and territorial governments. It seeks to foster public-private partnerships as a primary tool for enhancing resilience and addressing security threats. However, this reliance on voluntary partnerships reveals the same underlying issues seen in election infrastructure governance—namely, a permissive approach that prioritizes cooperation over accountability. The absence of binding commitments from stakeholders creates a fragmented system where security efforts are inconsistent and often reactive.

One of the central elements of the charter is its focus on information sharing. The document underscores the role of mechanisms like the **National Coordinating Center for Communications (NCC)** in facilitating communication between stakeholders. While this emphasis on shared intelligence is valuable, it does little to address the root causes of systemic vulnerabilities. Information sharing without enforcement mechanisms or mandated actions leads to a cycle of awareness without accountability, where risks are identified but not adequately mitigated.

The communications sector's role as an enabler for other critical infrastructure sectors adds another layer of complexity. As the backbone for data transmission and connectivity, any vulnerabilities in this sector can cascade across other sectors, amplifying risks. For example, election infrastructure relies heavily on secure and resilient communications systems for data transmission, reporting, and coordination. Despite this critical interdependency, the charter does not integrate mandates like **Executive Order 13800** or the **NIST Cybersecurity Framework**, which are designed to enforce rigorous standards for critical infrastructure protection.

The charter's reliance on advisory mechanisms highlights a broader trend in critical infrastructure governance, where agencies provide recommendations without enforcing compliance. While the **Cybersecurity and Infrastructure Security Agency (CISA)** operates solely in an advisory capacity with no legal enforcement authority, the

National Institute of Standards and Technology (NIST) occupies a unique position. Although **NIST** is also an advisory agency by design, its **NIST Cybersecurity Framework (CSF)** has been granted enforceability through **Executive Order 13800,** which makes adherence to its guidelines a federal requirement for critical infrastructure sectors, including elections. This distinction is crucial: **CISA's** recommendations remain entirely voluntary, while **NIST's CSF,** under **EO 13800**, imposes a legal obligation to meet its standards. The failure to enforce compliance with **NIST's** federally-backed guidelines exacerbates systemic vulnerabilities, as vendors and state agencies exploit this lack of accountability, perpetuating risks in sectors such as election infrastructure.

Another critical oversight in the charter is its failure to address vendor dependencies comprehensively, even with the involvement of the **National Institute of Standards and Technology (NIST)** as a guiding entity. The communications sector, much like election infrastructure, relies heavily on private vendors for hardware, software, and services, which introduces significant risks. These include outdated technologies, exploitable vulnerabilities, and a lack of transparency in vendor operations. While the charter references collaboration with entities like **NIST**, it does not enforce adherence to the **NIST Cybersecurity Framework (CSF)**, despite its clear authority under **Executive Order 13800**. This omission allows critical vulnerabilities tied to vendor dependencies to persist unchecked, leaving the sector exposed to preventable risks.

The lack of enforcement mechanisms is particularly alarming given the stakes involved. Communications infrastructure forms the backbone for data sharing and connectivity across all critical infrastructure sectors, including healthcare, emergency services, and elections. Compromises in this sector could have cascading effects, disrupting interconnected systems nationwide. The permissive structure of the charter, which relies on voluntary participation and self-regulation, undermines the authority of the **NIST CSF** and fails to meet the accountability standards mandated under federal law. This permissiveness not only heightens systemic vulnerabilities but also represents a direct violation of the requirements established by **EO 13800**.

In the broader context of election security, the governance model outlined in this charter parallels the systemic failures seen in other critical infrastructure sectors. Both the communications and election systems sectors are hindered by a reliance on voluntary compliance and advisory mechanisms. However, the critical difference here lies in the involvement of **NIST**. While advisory bodies like **CISA** lack enforcement authority, **NIST's CSF** is backed by federal law under **EO 13800**, making its standards legally

binding for critical infrastructure. The failure to enforce these standards in the communications sector reflects a broader neglect of federal cybersecurity mandates and undermines the integrity of the entire critical infrastructure ecosystem.

The "**Communications Government Coordinating Council Charter"** reveals systemic deficiencies in critical infrastructure governance that are particularly damning given the inclusion of **NIST's** legally enforceable framework. By failing to mandate compliance with the **NIST CSF,** the charter not only compromises the resilience of the communications sector but also highlights a broader reluctance to enforce accountability across interconnected systems, including elections. Addressing these issues requires a shift from permissive governance models to frameworks that enforce federal mandates, hold vendors accountable, and prioritize independent oversight. Without such reforms, the resilience and integrity of critical infrastructure will remain at risk, leaving the nation vulnerable to both systemic failures and external threats.

communications-gcc-charter-2020-508.pdf

https://docdro.id/9XIGzMV

The Help America Vote Act (HAVA)

The Help America Vote Act (HAVA) of 2002 brought about significant changes to the administration of elections in the United States, including the establishment of the **Election Assistance Commission (EAC)**. While the creation of the **EAC** was intended to improve election systems and promote best practices nationwide, its authority is notably limited. The **EAC** is fundamentally an advisory body, tasked with serving as a clearinghouse for election-related information and procedures. It inherited much of its role from the **Federal Election Commission's Office of Election Administration**, aiming to provide resources and guidance to state and local election officials. However, this advisory role lacks the enforcement power necessary to address systemic issues effectively.

A central aspect of the **EAC's** mission is the development of ***Voluntary Voting System Guidelines (VVSG)***. These guidelines are intended to provide a national standard for the security, functionality, and accessibility of voting systems. However, as the name suggests, the guidelines are not mandatory. States are free to adopt them, modify them, or ignore them entirely. Similarly, the **EAC** oversees the accreditation of laboratories

that test voting systems, but even this certification process is optional. Without a legal mandate to enforce these standards, the **EAC's** efforts rely on the willingness of states and vendors to voluntarily comply. This creates a fragmented system where the quality and security of voting systems vary significantly across jurisdictions.

The limitations of the **EAC** are further underscored by its lack of regulatory authority. **HAVA** explicitly prohibits the **EAC** from issuing rules or imposing requirements on states and localities, with the exception of some minimal oversight tied to the administration of funds allocated under the Act. This restriction means that the **EAC** cannot compel compliance with the guidelines or hold jurisdictions accountable for failing to meet certain benchmarks. Instead, it functions as a facilitator, providing resources and funding for election improvements but lacking the tools to ensure these resources are used effectively or uniformly.

Funding oversight is one of the **EAC's** primary roles. **HAVA** allocated substantial federal funds to improve voting systems, enhance accessibility, and modernize election processes. While the **EAC** oversees the distribution of these funds, it does not have the authority to enforce how states implement these improvements. This lack of enforcement creates a system where states may adopt inconsistent practices, some of which may not meet the highest standards of security or functionality.

The **EAC's** reliance on voluntary compliance is emblematic of broader issues in critical infrastructure governance. While the **EAC** provides valuable resources and guidance, its inability to mandate compliance creates vulnerabilities in the election system. For example, the voluntary nature of the **VVSG** means that some jurisdictions may choose not to adopt the latest security measures, leaving their systems exposed to risks. This contrasts sharply with frameworks like the **NIST Cybersecurity Framework** under **Executive Order 13800**, which impose enforceable requirements for critical infrastructure sectors, including elections. The absence of similar enforceability for the **EAC’s** guidelines undermines the uniformity and security of election systems.

Additionally, the **EAC’s** structure as an advisory body makes it ill-equipped to address modern election security challenges. The voluntary nature of its guidelines and the lack of mandatory oversight mechanisms result in a system that is reactive rather than proactive. While the **EAC** can identify vulnerabilities and recommend solutions, it cannot compel action to mitigate these risks. This dynamic perpetuates a fragmented

election security landscape where vulnerabilities persist unchecked in some areas, potentially compromising the integrity of the entire system.

The reliance on voluntary measures also limits transparency and accountability. Without a mandate to enforce compliance or conduct audits, the **EAC** cannot ensure that states or vendors are adhering to best practices. This lack of oversight allows systemic issues to go unaddressed and leaves the door open for inconsistencies and potential vulnerabilities in election administration.

In conclusion, the **EAC's** role under **HAVA** highlights the limitations of an advisory framework in addressing the complexities of election security. While the **EAC** provides valuable resources, its lack of enforcement authority diminishes its ability to ensure the uniform application of best practices across the nation. The reliance on voluntary compliance, coupled with the absence of mandatory oversight mechanisms, leaves significant gaps in the security and functionality of election systems. This structure, while beneficial in fostering collaboration, ultimately undermines the accountability and resilience needed to protect the integrity of U.S. elections.

HAVA.pdf

https://docdro.id/npWfW2V

Trade Secrets Act (18 U.S.C. § 1905)

The **Trade Secrets Act**, which governs the handling of proprietary information by federal agencies, has been consistently misinterpreted and misused to justify a lack of transparency in election security and critical infrastructure management. A detailed analysis of the statute reveals that while it does indeed protect trade secrets from unauthorized disclosure, it contains an explicit exception: disclosures are permissible when **required by law**. This exception is pivotal in countering claims that federal agencies, such as **CISA** and the **EAC**, can use the **Trade Secrets Act** as a shield to withhold information critical to public and national security.

The Act's central premise is to safeguard confidential commercial information, ensuring businesses are not unfairly disadvantaged by their interactions with government entities. However, the clause allowing disclosures under legal compulsion fundamentally alters the dynamic when laws like **Executive Order 13800** and the **NIST Cybersecurity**

Framework (CSF) come into play. **EO 13800** explicitly mandates robust transparency and accountability measures for critical infrastructure, including election systems. It requires adherence to the **NIST CSF**, which includes specific controls for maintaining transparency and mitigating cybersecurity risks.

Under these requirements, any claims that proprietary information about voting systems, software dependencies, or vulnerabilities cannot be disclosed due to the **Trade Secrets Act** lack merit. The "binding by law" clause in the **Trade Secrets Act** makes it clear that where federal mandates require such transparency—as **EO 13800** does—the Act cannot be used to withhold information. This directly contradicts the narrative advanced by agencies like **CISA** and organizations such as the **NASS** and **NASED**, which have propagated the notion that proprietary software or security vulnerabilities are shielded from disclosure under the Act.

Moreover, the absence of enforcement mechanisms and the reliance on voluntary compliance in the frameworks advanced by the **EAC** and **CISA** exacerbate these issues. By positioning themselves as advisory entities without regulatory power, these agencies create a façade of security that sidesteps the legal obligations of **EO 13800**. The reliance on the **Trade Secrets Act** to justify non-compliance further compounds this issue, presenting a significant barrier to public accountability and national security.

A deeper issue emerges in how the interpretation of the **Trade Secrets Act** undermines the foundational principles of transparency, safety, and security mandated by federal law. For example:

- **Transparency:** The refusal to disclose third-party software dependencies or known vulnerabilities prevents the public and independent bodies from evaluating the true state of election security. This lack of transparency erodes trust in the electoral process.
- **Safety:** Without disclosure, vulnerabilities remain hidden, leaving systems exposed to exploitation. The lack of independent third-party audits exacerbates this risk, as agencies and vendors effectively self-regulate without external accountability.
- **Security:** The conflation of protecting trade secrets with withholding critical cybersecurity information weakens overall security. It prioritizes corporate interests over national security imperatives, contrary to the intent of **EO 13800** and the **NIST CSF.**

In conclusion, the misuse of the **Trade Secrets Act** by **CISA**, the **EAC**, and other stakeholders to withhold critical election security information is a clear violation of the principles enshrined in **EO 13800** and the **NIST CSF**. These frameworks are legally binding and explicitly require transparency and independent accountability. By failing to adhere to these mandates, these agencies and their partners not only violate federal law but also compromise the integrity of the nation’s critical infrastructure. This issue demands immediate attention to ensure compliance with the law and to safeguard the transparency and security of critical systems.

trade_secrets_act.pdf

https://docdro.id/BrmrtLp

Extinguishing the wildfire of lies spread across the United States

Election Security Rumor vs. Reality - CISA

The **"Election Security Rumor vs. Reality"** document, released by **CISA**, serves as a public-facing attempt to address widespread concerns about the security and integrity of U.S. elections. Framed as a myth-busting guide, the file seeks to dismiss several pressing questions and doubts raised by voters, election officials, and security experts as mere "rumors." However, upon closer scrutiny, many of the so-called "realities" presented in the document rely on misleading narratives, half-truths, and omissions.

Rather than providing transparency and clarity, this document appears to perpetuate a carefully crafted narrative designed to obscure systemic vulnerabilities, deflect accountability, and bolster public confidence in systems that, as our investigation reveals, are fraught with weaknesses. From network connectivity concerns to the role of third-party vendors and the lack of enforceable federal standards, the issues dismissed as "rumors" often align closely with documented realities.

This analysis will delve into these claims, dissecting **CISA's** narrative and contrasting it with the findings of this investigation. By exposing the discrepancies between their "realities" and the evidence, we aim to illuminate the critical flaws in the current election security framework, highlight the failure to adhere to federal mandates such as **EO 13800**, and underscore the need for true accountability and transparency in protecting the nation’s electoral processes.

Key Questions for Analysis:

1. **Rumor**: Voting systems are connected to the Internet, leaving them vulnerable to hacking.
2. **Rumor**: There is no meaningful oversight or accountability in election system certification.
3. **Rumor**: Election systems rely heavily on third-party software, creating unaddressed vulnerabilities.
4. **Rumor**: Voting systems lack meaningful transparency, with critical information withheld under "trade secrets."
5. **Rumor**: Federal agencies enforce election security requirements.
6. **Rumor**: The NIST Cybersecurity Framework is not applicable to election systems.

Rumor: Voting systems are connected to the Internet, leaving them vulnerable to hacking

The narrative that voting systems are entirely disconnected from the Internet, rendering them immune to hacking, is a persistent claim by federal agencies like **CISA** and election system vendors. However, evidence from documentation, investigative findings, and vendor manuals exposes this claim as not only misleading but also dangerously simplistic. Far from being isolated, these systems and their supporting infrastructure frequently rely on interconnected technologies and networked environments, creating vulnerabilities that compromise the integrity and security of election systems. These vulnerabilities highlight a systemic failure to ensure compliance with federal mandates and robust cybersecurity standards.

Election systems are deeply interconnected. Beyond the voting machines themselves, these systems include voter registration databases, electronic poll books, tabulation machines, and reporting systems. Each of these components often interacts with networked environments. For instance, voter registration databases and poll books frequently rely on cloud services or centralized systems for real-time updates, which are inherently network-connected. Similarly, many jurisdictions use modems to transmit unofficial election results to central servers, further complicating the narrative of complete isolation.

Vendor documentation unequivocally demonstrates these dependencies. In the prior analysis, the ***Clear Ballot ClearCount Election Preparation and Installation Guide***

detailed how Ethernet-based networks are integral to the synchronization of tabulators, scanners, and centralized servers. The ***Hart Verity System Guide*** revealed browser-based management tools reliant on local IP networks. Even systems claiming to operate in air-gapped configurations, such as ***ES&S Electionware,*** rely on shared servers and networked devices for their functionality. These dependencies undermine claims of absolute isolation.

A specific point of failure involves the use of ***intranet-style configurations.*** While marketed as "closed networks," these systems depend on **routers, switches, and commercial off-the-shelf (COTS) components,** all of which are susceptible to misconfiguration or exploitation. Moreover, the use of tools like ***RSYNC*** for data synchronization introduces potential vulnerabilities, as such tools rely on standardized protocols that can be targeted by attackers if not properly secured.

The reliance on removable media, such as **USB drives**, is another critical vulnerability. Although touted as a method to maintain physical separation, **USB drives** can easily transfer malware between systems if chain-of-custody protocols are weak. This creates opportunities for attackers to introduce malicious code, particularly when these drives are used in environments lacking robust scanning and verification procedures.

Federal and state agencies exacerbate these issues by obstructing transparency and third-party assessments. The refusal to release cast vote records (CVRs) and related audit materials under the guise of "security" further shields vulnerabilities from scrutiny. This lack of accountability directly violates **EO 13800,** which mandates transparency and adherence to the **NIST CSF** for critical infrastructure. Instead of complying with these federal laws, agencies like **CISA** have advised states to restrict public access, citing misinterpreted concerns under the **Trade Secrets Act**—a claim invalidated by the legal requirement for federal transparency when national security is at stake.

The findings of ***"Exposing the Connectivity Risks"*** reinforce these points by documenting how election systems' operational configurations fail to meet federal cybersecurity standards. Vendors’ manuals and state operational guides collectively expose a reliance on networked environments and proprietary technologies, which are inherently vulnerable to exploitation. These vulnerabilities are not speculative; they represent a documented failure to secure critical infrastructure as mandated by federal law.

Despite **CISA** and the **EAC's** promotion of voluntary guidelines and best practices, their failure to enforce the **NIST CSF** and **EO 13800** underscores systemic negligence. This inaction not only leaves election systems exposed to cyber threats but also erodes public trust in the democratic process. The illusion of security perpetuated by claims of air-gapped systems must be dismantled with transparency, accountability, and adherence to federal mandates.

The claim that voting systems are not connected to the Internet is a deceptive simplification that obscures the true vulnerabilities of the election infrastructure. These systems, reliant on ***intranet-style configurations, networked devices,*** and ***external dependencies,*** are far from immune to cyber threats. The systemic refusal to acknowledge and address these risks is a violation of federal law and a direct threat to national security, demanding immediate corrective action to safeguard the integrity of U.S. elections.

Rumor: There is no meaningful oversight or accountability in election system certification

The claim that there is "meaningful oversight and accountability" in election system certification is a cornerstone of the federal narrative, primarily advanced by agencies like the **Election Assistance Commission (EAC)** and supported by **CISA**. However, this investigation has thoroughly dismantled the illusion of oversight and accountability in the current certification process, exposing it as a voluntary, ineffective, and largely symbolic framework that fails to meet the stringent requirements of federal law.

The **EAC**, established under the **Help America Vote Act (HAVA)** of 2002, is often presented as the authority overseeing election system certification. However, **HAVA** does not grant the **EAC** regulatory or enforcement powers. Instead, the **EAC** operates within an entirely voluntary framework. Voting system vendors can choose whether or not to submit their systems for testing and certification through **EAC**-approved laboratories. These certifications are often touted as a seal of approval, but their voluntary nature means that non-compliance carries no legal or practical consequences. In fact, several jurisdictions across the United States use election systems that have not undergone **EAC** certification, undermining the claim of universal oversight.

Further, the certification process itself lacks rigor and transparency. The testing conducted by **EAC**-accredited laboratories does not include independent third-party

audits or comprehensive assessments aligned with the **NIST Cybersecurity Framework (CSF)**, as required under **EO 13800** for critical infrastructure. Instead, the process relies heavily on vendor-supplied documentation and self-reported compliance, creating a conflict of interest that compromises the integrity of the certification. This voluntary, vendor-driven model stands in stark contrast to the independent oversight and mandatory compliance testing outlined in **EO 13800.**

The lack of accountability extends to the role of third-party dependencies within voting systems. Vendors like **Dominion Voting Systems, ES&S**, and **Hart InterCivic** integrate third-party software and hardware components, yet these dependencies are not independently tested during the certification process. This omission allows vulnerabilities in third-party components—such as outdated libraries, exploitable code, or unpatched software—to go undetected and unaddressed. The absence of accountability for these dependencies further exposes election systems to significant security risks.

CISA's endorsement of the **EAC** certification process as a cornerstone of election security is deeply problematic. By promoting this voluntary framework as a robust security measure, **CISA** not only misleads the public but also deflects attention from its failure to enforce the federal mandates outlined in **EO 13800**. This executive order requires rigorous risk management protocols and independent assessments for all critical infrastructure, including election systems. Yet, **CISA** and the **EAC** have constructed a parallel narrative that bypasses these requirements, allowing election officials and vendors to avoid meaningful accountability.

The narrative of oversight is further undermined by the lack of transparency in the certification process. Requests for information about vulnerabilities in certified systems are often denied under the guise of protecting "trade secrets," despite the clear legal mandate for transparency in **EO 13800** and the **NIST CSF**. This refusal to disclose critical information not only violates federal law but also erodes public trust in the electoral process.

In practice, the current certification process provides a veneer of legitimacy while allowing systemic vulnerabilities to persist. The absence of enforceable standards, the reliance on vendor-driven documentation, and the exclusion of independent audits combine to create a system that is neither accountable nor secure. The public is left with

the false impression that certified systems are rigorously tested and safe, when in reality, the process lacks the integrity needed to ensure election security.

The claim of meaningful oversight and accountability in election system certification is a carefully constructed fiction. The **EAC's** voluntary framework, the lack of independent audits, and the systemic evasion of federal mandates like **EO 13800** reveal a certification process that is fundamentally inadequate. This failure not only jeopardizes the security of election systems but also undermines public confidence in the democratic process. True oversight and accountability can only be achieved through mandatory compliance with federal cybersecurity standards, independent assessments, and full transparency—none of which are present in the current system.

Rumor: Election systems rely heavily on third-party software, creating unaddressed vulnerabilities

CISA dismisses concerns about election systems' reliance on third-party software and its associated risks as a "rumor," claiming that such dependencies are sufficiently managed through testing and certification. However, this investigation reveals that third-party software dependencies are a substantial and persistent vulnerability in election systems. The lack of rigorous oversight, transparency, and independent verification has allowed these risks to remain unaddressed, directly contradicting **CISA's** assertions.

Election system vendors such as **Dominion Voting Systems, ES&S,** and **Hart InterCivic** frequently rely on third-party components to operate their hardware and software. These dependencies include ***commercial off-the-shelf (COTS)*** software, third-party libraries, and hardware sourced from external manufacturers. While these components are integral to the functioning of election systems, they are not subject to independent, comprehensive testing during the certification process. Instead, the **EAC** and its accredited laboratories rely on documentation provided by the vendors themselves, creating a significant gap in accountability.

One critical issue with third-party dependencies is the lack of transparency regarding their security. Proprietary software and hardware are often shielded from public scrutiny under the guise of protecting intellectual property or trade secrets. This lack of transparency prevents independent experts from assessing the integrity of the components used in election systems. Furthermore, vendors are not required to disclose whether their systems incorporate outdated or vulnerable third-party software, such as

unpatched libraries or deprecated codebases. This omission leaves systems exposed to known exploits that could be leveraged by malicious actors.

The reliance on third-party software is particularly concerning given the documented history of supply chain attacks. High-profile incidents such as the ***SolarWinds breach*** demonstrate how attackers can compromise widely used third-party components to infiltrate critical systems. Election systems are not immune to these risks. For example, if a third-party library used in voting machine software is compromised, it could introduce vulnerabilities that jeopardize the integrity of election results. The absence of robust third-party auditing and compliance testing exacerbates these risks, as vulnerabilities remain undetected and unmitigated.

CISA's narrative that testing and certification adequately address these vulnerabilities is fundamentally flawed. As outlined in **EO 13800**, critical infrastructure sectors, including election systems, are required to comply with the **NIST Cybersecurity Framework (CSF)**. This framework emphasizes the importance of identifying and mitigating risks associated with third-party dependencies. Yet, the voluntary nature of the **EAC's** certification process means that these requirements are often ignored or superficially addressed. Vendors are not held accountable for ensuring the security of third-party components, and election officials are left to operate systems with unknown vulnerabilities.

Further compounding the issue is the reliance on cloud-based services for election data storage and management. Platforms like **Microsoft Azure** are used to store voter registration databases, ballot images, and cast vote records. While cloud services offer scalability and convenience, they also introduce single points of failure and expand the attack surface. The security of these platforms depends not only on the service provider but also on the integrity of the third-party software used within the cloud environment. Without independent oversight, these risks remain inadequately addressed.

The lack of independent third-party audits is a glaring omission in the election security framework. Independent assessments are essential for verifying the integrity of third-party software and ensuring that vulnerabilities are identified and mitigated. However, vendors and federal agencies have consistently resisted such audits, often citing the **Trade Secrets Act** to avoid disclosure. This refusal to allow transparency directly violates the mandates of **EO 13800**, which prioritize accountability and risk management in critical infrastructure.

The claim that third-party software dependencies are adequately managed in election systems is demonstrably false. The reliance on proprietary components, the lack of transparency, and the absence of independent verification create a system rife with vulnerabilities. **CISA's** dismissal of these concerns as a "rumor" serves to obscure the systemic failures that jeopardize the integrity of U.S. elections. To ensure secure and trustworthy elections, it is imperative to enforce federal mandates for transparency, third-party audits, and compliance with the **NIST CSF**—none of which are currently being upheld.

Rumor: The NIST Cybersecurity Framework is not applicable to election systems

CISA's acknowledgment that the **NIST Cybersecurity Framework (NIST CSF)** applies to election systems represents a truth in principle, but their actions betray a stark contradiction. While **CISA** publicly supports the applicability of the **NIST CSF** as a guiding framework for election infrastructure security, their practical initiatives have not upheld the federal mandates outlined in **EO 13800**. Instead, **CISA** has propagated policies and guidance that prioritize election system security and proprietary concerns of vendors over the critical balance of transparency, safety, and accountability mandated by federal law.

The **NIST CSF** is the sole cybersecurity framework enforceable under **EO 13800**, making it the only standard to which federal and state entities can be held accountable for securing critical infrastructure. Unlike **CISA's** purely advisory role, the **NIST CSF** provides enforceable guidelines that can result in **Department of Justice (DOJ)** enforcement actions if violated. This legal enforceability makes the **NIST CSF** the cornerstone of cybersecurity accountability for election systems, demanding independent assessments, transparent risk management, and compliance at every level. Yet, **CISA's** actions consistently subvert these objectives.

CISA's promotion of the **Trade Secrets Act** as justification for states and vendors to withhold critical information from public scrutiny is emblematic of this subversion. The **Trade Secrets Act** explicitly allows exceptions when compliance with law demands disclosure. The **NIST CSF**, mandated by **EO 13800**, is that legal requirement. By advising states and election vendors to withhold information about vulnerabilities or system dependencies under the guise of ***"trade secrets,"*** **CISA** not only undermines

federal law but also actively obstructs the transparency required to ensure the integrity of election systems.

This dynamic is further exacerbated by **CISA's** promotion of risk-limiting audits (RLAs). While RLAs are marketed as tools to enhance election security, they have enabled states to justify the restriction of cast vote records (CVRs) and other election-related data. The process relies heavily on chain-of-custody protocols that make every ballot identifiable through sequential imprinting, thereby destroying the anonymity of the vote—a fundamental human and constitutional right. This infringement violates the very principles the **NIST CSF** seeks to uphold: ensuring security, transparency, and trust without compromising voter privacy.

CISA's recommendations to restrict even seemingly innocuous public records further illustrate their role as architects of nationwide election opacity. By framing transparency as a "security risk," **CISA** perpetuates a false narrative that conceals systemic vulnerabilities, many of which directly violate **EO 13800** and the **NIST CSF**. If election systems were genuinely secure and compliant with federal mandates, transparency would not pose a threat. Instead, the push to limit public access underscores a deep-seated issue: widespread non-compliance with cybersecurity standards and a willful failure to address vulnerabilities.

CISA's role extends beyond negligence or even willful negligence. Their dissemination of mis-, dis-, and malinformation positions them as the central entity enabling nationwide violations of transparency, accountability, and election integrity. Through their carefully curated messaging, **CISA** has cultivated the perception of authority, misleading the public, state officials, and legislators into believing their guidelines carry regulatory or enforcement weight. This deception has facilitated the systematic erosion of constitutional protections, FOIA rights, and the integrity of federal and state cybersecurity laws.

The consequences of **CISA's** actions are far-reaching. By allowing the subversion of federal mandates, **CISA** has enabled state legislatures to pass laws in direct violation of the **Supremacy Clause**, obstructing compliance with **EO 13800**. Their guidance has empowered secretaries of state and election directors to restrict critical information under the pretense of security, despite the **NIST CSF's** explicit emphasis on transparency. Furthermore, **CISA's** influence has emboldened election vendors to

operate without independent scrutiny, perpetuating vulnerabilities and undermining public trust.

CISA's role as the messaging authority at the nexus of the **DHS**, state election agencies, and private vendors positions them as the linchpin in a covert effort to subvert national security under the guise of election security. Their deliberate obfuscation of federal mandates, coupled with their alignment with vendors and advisory entities like the **EAC**, represents not just a betrayal of their advisory responsibilities but a coordinated effort to undermine the cybersecurity framework that is the foundation of critical infrastructure protection.

This betrayal is not accidental. It reflects a calculated strategy to erode the sovereignty of U.S. election systems, bypass accountability mechanisms, and centralize control under a framework of voluntary compliance. By spreading misinformation that contradicts **EO 13800** and the **NIST CSF** while masking systemic vulnerabilities, **CISA** has created a clear and present danger to national security. This conduct, when examined in its entirety, aligns with the legal thresholds for willful negligence, intent to mislead, and aiding and abetting actions that weaken the United States' critical infrastructure—a potential foundation for charges of conspiracy and treason under the law.

While **CISA** publicly acknowledges the applicability of the **NIST CSF** to election systems, their actions reveal a stark contradiction. By prioritizing proprietary concerns and propagating false narratives, they have created a system of vulnerability and opacity that directly violates federal mandates. **CISA's** conduct demands accountability, not only for their role in undermining election security but for the broader implications of their actions on national sovereignty and public trust.

Rumor: Voting systems lack meaningful transparency, with critical information withheld under "trade secrets."

The claim that concerns over a lack of transparency in voting systems are mere rumors is deeply misleading. While **CISA** acknowledges the importance of transparency, its actions—alongside those of state election officials and private vendors—demonstrate a systematic effort to obscure critical information under the guise of "trade secrets." This practice not only undermines public trust but also conflicts with federal mandates designed to ensure both transparency and accountability in critical infrastructure, including elections.

At the heart of this issue is the misuse of the **Trade Secrets Act**. While the act protects proprietary information, it includes explicit exceptions requiring disclosure when mandated by law. Both **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)** demand transparency and rigorous security practices for critical infrastructure. These federal directives supersede trade secret protections when they obstruct the safeguarding of national security and the public interest. Yet, **CISA** and election officials have consistently cited trade secret concerns to block access to vital election data, including cast vote records (CVRs) and information about third-party software dependencies.

This practice is particularly concerning in the context of risk-limiting audits (RLAs). While RLAs are presented as a tool for enhancing election security, they rely on proprietary systems that are shielded from public scrutiny. Sequential ballot imprinting, a key feature of RLAs, creates a tracking system that theoretically enables the linkage of a ballot to a voter. This undermines the anonymity of the vote—a cornerstone of democratic elections—while the lack of transparency around these systems prevents public verification of their integrity.

The refusal to release CVRs exemplifies the broader issue of withheld transparency. CVRs, which contain anonymized voting data, are critical for public verification of election results. Denying access to these records under the pretense of protecting trade secrets not only violates the principles of transparency but also erodes public confidence in the electoral process. If election systems are truly secure, transparency should bolster trust, not threaten it.

Moreover, this lack of transparency extends to vendor operations. Private companies like **Dominion Voting Systems, ES&S,** and **Hart InterCivic** provide the hardware and software that underpin election infrastructure, yet their practices remain shielded from scrutiny. The refusal to subject these systems to independent third-party audits—a requirement under **EO 13800**—allows vulnerabilities to persist unchecked. This reliance on vendor self-assessments is not only insufficient but also directly undermines the federal standards designed to secure critical infrastructure.

The implications of this secrecy are far-reaching. By normalizing the withholding of critical information, **CISA** and its partners have set a dangerous precedent that extends beyond election systems to other sectors of critical infrastructure. This approach fosters

a culture of opacity, where systemic vulnerabilities remain hidden from the public and unaddressed by authorities.

In reality, the lack of transparency in voting systems is not a rumor but a well-documented issue that poses significant risks to national security. The misuse of the **Trade Secrets Act** to justify this secrecy is both legally and ethically indefensible, particularly in the face of federal mandates requiring transparency and accountability. **CISA's** role in promoting this narrative highlights its complicity in perpetuating a flawed system that prioritizes vendor protection over public trust and election integrity.

Rumor: Federal agencies enforce election security requirements.

The claim that federal agencies enforce election security requirements is misleading in a nuanced and deliberately deceptive way. While agencies like the **Cybersecurity and Infrastructure Security Agency (CISA)** and the **Election Assistance Commission (EAC)** do not possess direct enforcement powers, their role as advisory bodies has been strategically weaponized by the **Department of Homeland Security (DHS)** to push federal overreach under the guise of "voluntary compliance." This setup has allowed **DHS** to evade accountability for systemic failures in election security while creating the illusion of non-coercive guidance.

CISA, as an advisory agency, provides cybersecurity recommendations and risk mitigation strategies that states and election officials are encouraged to adopt. Similarly, the **EAC's *Voluntary Voting System Guidelines (VVSG)*** and certification processes are nominally optional. States and vendors are under no legal obligation to adhere to these guidelines or seek **EAC** certification for their voting systems. However, framing these processes as voluntary obscures the indirect pressure exerted by **DHS** through these agencies. The illusion of choice is maintained while states are incentivized, or covertly coerced, into adopting the prescribed measures to gain access to federal grants, resources, or to avoid political repercussions.

The **EAC**, despite being an advisory body, plays a crucial role in this ecosystem. Its voluntary guidelines serve as a baseline that states often adopt to signal compliance with "best practices." Yet, the lack of mandatory enforcement authority means that states and vendors can implement these standards selectively or ignore them entirely. This undermines the credibility of the **EAC's** certification process, as uncertified systems can

still be marketed and deployed without legal consequences. However, **DHS's** indirect influence through **CISA** and its partnership with the **EAC** allows the federal government to retain a degree of control while maintaining plausible deniability of overreach.

CISA, in particular, operates as a critical intermediary for **DHS**, spreading its messaging and recommendations while shielding **DHS** from direct accountability. **CISA** has positioned itself as the primary public-facing entity for election security, crafting narratives that misrepresent its role as advisory and inflate its influence as a de facto regulatory body. This dynamic is further amplified by its partnerships with organizations like the **Center for Internet Security (CIS), EI-ISAC,** and **MS-ISAC**, which receive federal funding and report information back to **DHS** under the guise of national security data-sharing agreements. These organizations, in turn, disseminate **CISA's** messaging to states and localities, creating a feedback loop that reinforces **DHS's** agenda.

The trade secrets argument used to justify withholding critical election system information is another layer of this deception. The **Trade Secrets Act** does protect proprietary information but includes exceptions when disclosure is required by federal law. **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF),** which mandate transparency and independent verification for critical infrastructure, supersede these trade secret protections. Yet, **CISA** and the **EAC** advise states to uphold these secrecy claims, effectively bypassing **EO 13800** and the **NIST CSF**. This practice prioritizes vendor interests over public accountability, leaving election systems vulnerable to cyber threats while preventing voters from verifying the integrity of their elections.

Risk-limiting audits (RLAs), often promoted by **CISA** and adopted by states under **DHS's** indirect influence, further exemplify this systemic failure. RLAs were conceived with input from **DHS** personnel, ostensibly to enhance election security. However, their implementation has often led to greater secrecy rather than transparency. The use of sequential ballot imprinting, which tracks ballot batches for auditing purposes, introduces the potential for linking ballots to voters, undermining the anonymity of the vote. This system has been paired with digital and cloud-based storage solutions, such as those provided by **Microsoft Azure**, to centralize election data, creating single points of failure vulnerable to cyberattacks.

CISA and the **EAC** have also advised states to restrict access to cast vote records (CVRs) and other public records under the guise of protecting election security. These

restrictions have been justified as necessary to maintain the integrity of RLAs and other processes. Yet, these measures primarily serve to shield vulnerabilities and prevent public scrutiny, rather than addressing the underlying security issues. The result is a system that prioritizes secrecy over the transparency mandated by **EO 13800** and the **NIST CSF**, directly violating federal law.

It is essential to recognize **DHS's** central role in orchestrating this framework. While **CISA** and the **EAC** appear to operate independently, their actions align closely with DHS's broader strategy to consolidate control over election security without appearing to overreach. **DHS's** involvement in the creation and promotion of RLAs and its funding of organizations like **CIS** further illustrates its covert influence. By delegating these responsibilities to advisory bodies, **DHS** insulates itself from criticism while ensuring that its agenda is implemented at the state and local levels.

The Department of Justice (DOJ) holds the enforcement authority necessary to address these systemic failures. **Under EO 13800**, state election officials and vendors are required to comply with the **NIST CSF** as part of critical infrastructure protections. Violations of these mandates, particularly those involving the misuse of trade secrets protections or the refusal to adhere to independent audit requirements, fall under the **DOJ's** jurisdiction. The narrative that state election officials are immune to federal prosecution for these violations is false. They are accountable under the **Supremacy Clause**, which ensures that federal law takes precedence over conflicting state actions.

The claim that federal agencies enforce election security requirements is a half-truth designed to mislead the public. While **CISA** and the **EAC** lack direct enforcement powers, they act as conduits for **DHS's** agenda, exerting indirect pressure on states and vendors. This strategy has enabled widespread non-compliance with **EO 13800** and the **NIST CSF,** creating systemic vulnerabilities that compromise election security. The **DOJ** must step in to hold these actors accountable, enforcing the federal mandates that have been systematically undermined by this deceptive and highly coordinated framework.

Election Security Rumor vs. Reality _ CISA.pdf

https://docdro.id/1m0sY8L

NASS/NASED FAQs

The **National Association of Secretaries of State (NASS)** FAQ document presents itself as a trusted resource for addressing public concerns about election security and administration. However, a closer examination reveals significant gaps and misrepresentations. Like the **CISA *"Rumor vs. Reality"*** document, the **NASS FAQs** aim to dismiss valid concerns while perpetuating narratives that align with their agenda of maintaining opacity and centralized control over election processes. This investigation focuses on exposing the inaccuracies and half-truths in the **NASS FAQs,** using evidence gathered through our broader inquiry into election system vulnerabilities, federal compliance requirements, and advisory agency overreach.

In this section, we will address questions from the **NASS FAQs** that have not been fully covered in our response to the **CISA *"Rumor vs. Reality***" document. These questions reveal distinct facets of misinformation and offer an opportunity to expand our critique of the mechanisms undermining election transparency and security.

Questions Not Yet Addressed:

1. How are voting machines certified, and what is the role of federal and state governments in certification?
2. Are voter registration databases vulnerable to hacking?
3. Is voting by mail secure?
4. Why aren’t cast vote records (**CVRs**) available to the public?
5. What steps are taken to ensure ballot security during the election process?
6. Do voting systems use outdated software?
7. Are election officials required to comply with federal cybersecurity standards?
8. How do election officials prevent unauthorized access to voter data?
9. What happens if there is evidence of a cyberattack on election infrastructure?

How are voting machines certified, and what is the role of federal and state governments in certification?

The process of certifying voting machines is often portrayed as a rigorous and multi-layered system involving both federal and state oversight. However, a closer look at the roles of the federal and state governments in certification reveals significant gaps in accountability and enforcement, rendering this system more symbolic than substantive.

At the federal level, the **Election Assistance Commission (EAC)** oversees the ***Voluntary Voting System Guidelines (VVSG)***, which set standards for voting systems. The **EAC** works with federally accredited laboratories to test and certify machines against these guidelines. However, as the name implies, the ***VVSG*** and the entire certification process are voluntary. States are not required to adopt the ***VVSG***, and vendors are not obligated to submit their systems for federal testing and certification. This voluntary framework undermines the credibility of the process, as uncertified systems can still be deployed without consequence.

Furthermore, the **EAC** lacks enforcement authority. Its role is limited to providing guidance and maintaining the accreditation of testing laboratories. This means that even if a voting system fails to meet the ***VVSG*** standards, the **EAC** cannot impose penalties or prevent its use in elections. This lack of regulatory power makes the federal certification process largely symbolic, leaving states to independently decide whether to require compliance.

At the state level, certification processes vary widely. Some states adopt the ***VVSG*** standards and require **EAC** certification, while others establish their own certification criteria or rely on self-assessments from vendors. This patchwork approach creates inconsistencies in the security and reliability of voting systems across the country. In many cases, states delegate significant authority to private vendors, allowing them to self-certify their compliance with state requirements. This reliance on vendor self-assessments introduces substantial risks, as it bypasses independent oversight and transparency.

The gaps in both federal and state certification processes are exacerbated by the proprietary nature of voting systems. Vendors often cite trade secret protections to avoid disclosing detailed information about their software and hardware. This lack of transparency prevents meaningful scrutiny of the systems' security and functionality, leaving vulnerabilities unaddressed. Moreover, the absence of mandatory third-party audits—required under the **NIST Cybersecurity Framework** and **EO 13800** for critical infrastructure—further weakens the certification process.

In conclusion, while the certification of voting machines is presented as a robust process involving federal and state collaboration, it is fundamentally flawed. The voluntary nature of federal guidelines, the lack of enforcement authority by the **EAC**, the inconsistent state-level requirements, and the reliance on vendor self-certifications

collectively create a system that fails to ensure the security and reliability of election systems. This inadequacy not only undermines public trust but also violates federal mandates designed to protect critical infrastructure, leaving the integrity of elections at risk.

Are voter registration databases vulnerable to hacking?

The question of whether voter registration databases are vulnerable to hacking is often met with assurances of robust security measures. However, the reality is far more complex. Evidence and investigations reveal that voter registration databases are indeed vulnerable, presenting a significant risk to the integrity of election systems.

Voter registration databases are part of the broader election infrastructure and often interact with various systems, including electronic poll books and centralized voter management platforms. These systems are frequently connected to networks, making them susceptible to cyberattacks. Common vulnerabilities include outdated software, insufficient access controls, and inadequate monitoring of network activity. These weaknesses have been exploited in past incidents, demonstrating that the risks are not hypothetical.

One of the most concerning aspects of voter registration database security is the lack of adherence to federally mandated cybersecurity frameworks. **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF)** require rigorous risk assessments, independent audits, and proactive mitigation strategies for critical infrastructure, including election systems. Despite these mandates, many states fail to implement these measures, leaving their systems exposed to cyber threats.

The 2016 election cycle provided a stark example of these vulnerabilities. Cyber actors targeted voter registration databases in multiple states, successfully accessing and ex-filtrating data in some cases. While these incidents did not result in direct manipulation of voter registration data, they exposed significant weaknesses in the security of these systems. The lack of transparency in how these breaches were addressed further undermines public trust in the integrity of voter registration databases.

Compounding these risks is the reliance on third-party vendors for managing voter registration databases. Many states contract private companies to develop and maintain these systems, often without requiring comprehensive security audits. Vendors frequently cite proprietary information as a reason for withholding detailed

documentation about their systems, creating a significant barrier to transparency and accountability. This reliance on vendor self-assessments leaves critical vulnerabilities unaddressed.

Cloud-based storage solutions, such as those provided by **Microsoft Azure**, introduce additional risks. While cloud platforms offer scalability and accessibility, they also create centralized points of failure that are attractive targets for cyberattacks. The use of cloud services in voter registration database management raises questions about the adequacy of security measures and compliance with federal mandates.

CISA's guidance on voter registration database security often focuses on incident response rather than prevention. While information-sharing platforms like the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** provide valuable resources, their advisory nature does not compel compliance with federally mandated standards. This reactive approach fails to address the systemic vulnerabilities that make voter registration databases prime targets for cyberattacks.

Voter registration databases are inherently vulnerable to hacking due to their network connectivity, reliance on third-party vendors, and lack of adherence to federal cybersecurity standards. These vulnerabilities are exacerbated by the absence of independent audits, inadequate transparency, and a reactive rather than proactive approach to security. Addressing these issues requires a commitment to enforcing the **NIST CSF** and **EO 13800**, implementing robust security measures, and ensuring accountability through transparency and independent oversight. Without these steps, the security of voter registration databases—and the integrity of elections—remains at risk.

Is voting by mail secure?

The question of whether voting by mail is secure must also address a critical and often overlooked issue: the potential for voter intimidation or undue influence within the home. While mail-in voting offers convenience and accessibility, it removes the safeguards of anonymity and privacy inherent in in-person voting at a polling station. This systemic flaw in mail-in voting undermines the principle of free and independent choice, a cornerstone of democratic processes and protected under constitutional, international, and human rights.

Mail-in voting relies on ballots being sent to voters' residences, where they are expected to fill them out independently and free from coercion. However, the state has no way to

verify whether this independence is maintained. In households where one individual, such as a parent or spouse, holds disproportionate influence, the opportunity for voter manipulation arises. For example, a father receiving six ballots for his household could potentially vote on all of them himself, marking each with his choices. If these ballots are later dropped off at a local dropbox, the system would have no mechanism to detect this fraud. In states where it is lawful for one family member to return multiple ballots to a dropbox, this potential for abuse is even greater.

The tracking mechanisms used for mail-in ballots, such as barcodes or QR codes that link a ballot to a specific voter's registration, focus only on logistical transparency—confirming that the ballot has been sent, received, and processed. These mechanisms, while useful for tracking the movement of a ballot, provide no assurance that the votes cast were made independently or reflect the individual conscience of each voter. The state can confirm that a ballot was returned but cannot confirm that it was filled out by the intended voter or without external pressure.

Voter manipulation is not limited to outright fraud. Subtle or overt coercion within the household is another significant concern. Family members may influence one another's votes, whether through persuasion, emotional pressure, or outright threats. For example, a parent with strong political views might insist that their children vote a certain way, threatening consequences such as disownment or eviction if their preferences are not followed. Around the dinner table, this coercion can easily transform into collective voting, where the secrecy and individuality of the voting process are entirely lost.

The propaganda-laden media environment exacerbates this issue. Since the passage of the **Smith-Mundt Modernization Act**, which permits the dissemination of government-funded messaging to domestic audiences, misinformation and divisive rhetoric have intensified. Families already fractured by political divisions are particularly susceptible to undue influence within the home. This environment undermines the ability of individuals to make free and independent choices, transforming the household into a battleground for political control rather than a sanctuary for individual conscience.

In-person voting at polling stations, with its private booths and enforced secrecy, inherently protects against these forms of voter manipulation. The controlled environment ensures that each voter has the opportunity to make their choices without external influence. Mail-in voting, by contrast, transfers responsibility for maintaining

this independence to the voter’s home environment, which cannot be adequately monitored or safeguarded by election officials.

Additionally, mail-in voting undermines the chain of custody for voter anonymity and privacy. By delivering ballots to private residences, the system introduces a vulnerability that allows for potential breaches of secrecy and independence. The constitutional guarantee of privacy in voting, along with international and human rights protections for free and independent elections, is violated at a systemic level under mail-in voting practices.

The state, counties, and the nation have no mechanisms to verify the conditions under which mail-in ballots are filled out. They cannot ascertain whether the votes cast reflect the independent will of the voters or if they were subjected to external pressures, threats, or manipulations. This systemic flaw renders mail-in voting inherently fraudulent, as it fails to protect the fundamental principles of privacy, independence, and anonymity essential to democratic integrity.

While mail-in voting can be secure in terms of logistical tracking and processing, it fails to address the critical vulnerabilities related to voter independence and privacy. The potential for manipulation within the household, coupled with the lack of safeguards to ensure anonymity, creates a process that is fundamentally flawed and open to abuse. These systemic issues undermine not only the integrity of mail-in voting but also the broader trust in democratic processes. Only by addressing these deficiencies can the true security and fairness of elections be ensured.

Why aren’t cast vote records (CVRs) available to the public?

The question of why **cast vote records (CVRs)** are not made publicly available is emblematic of deeper systemic issues within election transparency and security. State officials and federal advisory bodies such as **CISA** often argue that releasing **CVRs** could compromise voter privacy, especially in small precincts where unique voting patterns might reveal individual choices. They further claim that **CVRs**, as part of "election system security," could undermine the integrity of election systems if released. However, these justifications, while seemingly logical on the surface, fall apart under scrutiny and fail to address the larger implications of withholding these records.

First, **CVRs** are aggregated data that, when properly anonymized, do not contain personally identifiable information. In many sectors outside elections, anonymization techniques are standard practice to balance transparency and privacy. The argument that **CVRs** inherently pose a privacy risk is therefore misleading. Instead, this narrative appears to be a convenient excuse to obstruct public access to information that could otherwise allow independent verification of election outcomes.

The refusal to release **CVRs** also hides deeper systemic vulnerabilities in the election process, particularly those introduced by the Risk-Limiting Audit (RLA) system. RLAs, heavily promoted by **CISA**, academic institutions, and **NGOs**, involve detailed tracking and imprinting of ballots and envelopes to facilitate comparisons between physical paper ballots and their digital counterparts. The **ARLO** software, developed by **VotingWorks** and central to this process, enables election officials to locate specific ballots for audit purposes. While this is presented as a method to ensure accuracy, the underlying system creates a literal filing mechanism where the sequence and storage of ballots and envelopes can be cross-referenced.

This filing system, coupled with the use of cloud-based storage solutions like **Microsoft Azure**, introduces a significant risk to voter anonymity. When envelopes containing voter signatures and ballot style information are stored alongside their corresponding ballots in the cloud, they can theoretically be queried and linked. Such capabilities would allow government agencies, administrations, or any entity with access through federal information-sharing agreements to determine how individuals voted. This potential undermines the foundational principle of anonymous voting, a cornerstone of constitutional, international, and human rights.

The implications of this system extend far beyond mere administrative efficiency. It reveals a deliberate and systemic effort to conceal the vulnerabilities and privacy risks inherent in the RLA process. The refusal to release **CVRs** ensures that these issues remain hidden from public scrutiny, leaving voters unaware of the extent to which their privacy may be compromised. Moreover, the secrecy surrounding the imprinting and filing of ballots and envelopes shields the entities responsible for implementing these systems—ranging from federal advisory agencies like **CISA** and the **EAC** to state associations and private vendors—from accountability.

The justification for withholding **CVRs** also frequently invokes the **Trade Secrets Act**, which is used to claim that proprietary election system information cannot be disclosed.

However, this argument is fundamentally flawed when placed against the legal framework established by **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)**. These federal mandates require transparency, safety, and security as integral components of critical infrastructure protection, overriding any claims of trade secrecy that would otherwise obstruct compliance with federal law. The **Trade Secrets Act** itself provides exceptions for disclosures mandated by law, making this justification untenable in the context of election security.

Furthermore, the refusal to release **CVRs** not only violates federal mandates but also erodes public trust in the electoral process. Transparency is a critical component of democratic governance, and the ability for independent auditors, researchers, and the public to verify election outcomes is essential for maintaining confidence in the system. By withholding **CVRs**, state and federal officials create barriers to accountability, fostering a perception of secrecy and vulnerability that undermines the integrity of elections.

The broader context reveals that the adoption of RLAs and the corresponding restrictions on transparency are not isolated decisions. These measures have been systematically promoted by a network of federal agencies, academic institutions, vendors, and **NGOs**, often lobbying state legislatures and county associations to implement these practices. While presented as voluntary or advisory, the coordinated effort behind these systems demonstrates an intent to normalize a framework that prioritizes system security over voter privacy and transparency.

The refusal to release **CVRs** is a calculated decision designed to conceal the vulnerabilities and systemic risks inherent in the current election infrastructure. By invoking concerns over privacy and security, officials obscure the reality of a system that compromises both. The reliance on flawed justifications like the **Trade Secrets Act** and the concealment of risks associated with RLAs reflect a broader failure to align election processes with the principles of transparency and accountability mandated by federal law. The integrity of U.S. elections depends on addressing these issues openly and ensuring that transparency, security, and voter privacy are upheld without compromise.

What steps are taken to ensure ballot security during the election process?

The question of what steps are taken to ensure ballot security during the election process is critical to understanding the measures purportedly designed to safeguard electoral integrity. Official narratives from federal advisory bodies like **CISA** and state election offices emphasize chain-of-custody protocols, secure storage, and robust tracking mechanisms as essential components of ballot security. However, upon closer examination, these steps often fail to address—or even exacerbate—systemic vulnerabilities and privacy concerns inherent in the election process.

The chain-of-custody protocols, while publicly touted as a safeguard, are deeply intertwined with the Risk-Limiting Audit (RLA) process. These protocols include the imprinting of ballots and envelopes to track their location in storage, which, as previously noted, can compromise voter anonymity. By enabling precise retrieval of specific ballots based on their sequence in storage, these protocols inadvertently create a system that risks linking individual ballots back to voters when paired with other data sources, such as digital images stored in cloud systems.

Secure storage and transport mechanisms are another cornerstone of ballot security narratives. Election officials point to physical security measures like sealed ballot boxes, tamper-evident envelopes, and surveillance of storage facilities as evidence of robust security. While these measures are important, they do little to address vulnerabilities introduced during electronic transmission of data, particularly in systems that rely on networked environments or cloud-based storage for ballot tracking and reporting.

Ballot tracking mechanisms, which include barcodes and QR codes used to track mail-in ballots, also present a double-edged sword. While these tools enhance logistical efficiency and transparency for voters who wish to verify the status of their ballots, they also create a dataset that can be exploited if security measures fail. For example, malicious actors gaining access to this tracking data could potentially interfere with the election process by targeting specific ballots or disrupting the chain of custody.

Additionally, the reliance on third-party vendors for ballot printing, sorting, and tabulation introduces further risks. Vendors like **Dominion Voting Systems, ES&S, Hart InterCivic, Runbeck,** and **BlueCrest** play critical roles in the election process but often operate under limited transparency and accountability. The lack of independent third-party audits required under federal mandates like **EO 13800** and the **NIST Cybersecurity Framework (CSF)** leaves these systems vulnerable to exploitation. This

reliance on vendors also means that ballot security is only as strong as the weakest link in these proprietary systems.

A notable example of these risks is the use of mail-sorting and imprinting equipment by vendors like **Runbeck** and **BlueCrest**, which are integral to processing mail-in ballots. These systems often imprint ballots with unique identifiers as part of the sorting and auditing process. While ostensibly designed to enhance accuracy and security, this imprinting raises serious privacy concerns by enabling the potential linkage of ballots to voters, particularly when digital images of ballots and envelopes are stored together in cloud systems like **Microsoft Azure**.

Moreover, the lack of independent oversight or meaningful enforcement mechanisms exacerbates these vulnerabilities. Advisory agencies like **CISA** and the **EAC**, while instrumental in disseminating "best practices" and "voluntary guidelines," fail to align their frameworks with the stringent requirements mandated by federal law, such as those outlined in **EO 13800** and the **NIST Cybersecurity Framework (CSF)**. This disconnect renders their efforts not only ineffective but also noncompliant with the legal standards that govern critical infrastructure. Even if **CISA** and the **EAC** had the regulatory authority to enforce adherence to their recommendations—a power they currently lack—their voluntary voting guidelines and best practices fall woefully short of the comprehensive protections required by the **NIST CSF**. This inadequacy underscores their inability to fulfill the essential role of safeguarding election systems against systemic risks, leaving these vulnerabilities unchecked and undermining the integrity of the election process.

The steps taken to ensure ballot security during the election process often fall short of addressing the most significant vulnerabilities in the system. While chain-of-custody protocols, secure storage, and tracking mechanisms are critical components, they are insufficient in the absence of enforceable standards and independent oversight. The reliance on third-party vendors, the systemic risks introduced by networked and cloud-based systems, and the lack of transparency and accountability collectively undermine the integrity of ballot security. Addressing these issues requires a comprehensive reevaluation of the current framework to align it with the principles of transparency, security, and voter privacy mandated by federal law.

Do voting systems use outdated software?

Outdated software remains a persistent vulnerability within election systems, undermining their integrity and security. While federal agencies like **CISA** and the **EAC** offer guidelines and recommendations to mitigate risks, they have no enforcement authority to ensure compliance, leaving these vulnerabilities largely unaddressed. This investigation, supported by findings from the ***TLP:AMBER Election Infrastructure Cyber Risk Summary,*** reveals that outdated software and exploitable services often linger in election systems for extended periods—sometimes exceeding 400 days—without remediation. This failure to update critical systems violates federal cybersecurity mandates and exposes the electoral process to potential compromise.

Election jurisdictions often rely on vendors like **Dominion Voting Systems, ES&S,** and **Hart InterCivic** for software updates and maintenance. However, these updates are frequently implemented without independent third-party verification, allowing potential vulnerabilities to persist unchecked. Supply chain risks and third-party dependencies exacerbate these challenges, as malicious actors could exploit unverified software components to infiltrate critical systems. The reliance on vendor self-assessments, rather than adherence to the independent compliance measures required by **EO 13800** and the **NIST CSF**, further compounds this problem.

Under **EO 13800**, critical infrastructure sectors, including election systems, are required to align with the **NIST CSF** to ensure rigorous cybersecurity standards. The framework mandates periodic risk assessments, timely updates, and independent audits to identify and mitigate vulnerabilities. Yet, as the evidence shows, many election jurisdictions sidestep these requirements, relying instead on advisory agency recommendations that lack enforceability and fail to address systemic risks effectively.

The implications of using outdated software extend beyond technical vulnerabilities. They represent a fundamental failure of governance and accountability in election security. By not adhering to **EO 13800** and the **NIST CSF**, jurisdictions not only put their systems at risk but also violate federal law, which is enforceable by the **Department of Justice.** The persistence of outdated software reflects a broader neglect of the critical infrastructure standards designed to protect national security, eroding public trust in the electoral process.

CISA and the **EAC**, as advisory agencies, are not equipped to enforce compliance with federal mandates. Even if their guidelines were enforceable, they do not require strict adherence to the **NIST CSF**, rendering their efforts ineffective and unlawful. The

reliance on voluntary compliance and self-assessments creates a facade of security while allowing vulnerabilities to persist. This failure to address outdated software in election systems highlights the urgent need for transparency, independent oversight, and strict compliance with federally mandated cybersecurity standards to protect the integrity of U.S. elections.

Are election officials required to comply with federal cybersecurity standards?

Election officials are unequivocally bound by federal law to comply with cybersecurity standards as mandated by **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF).** These are not merely guidelines or advisory principles; they represent binding legal requirements for the security and integrity of critical infrastructure, including election systems. Any claims to the contrary, whether made by advisory agencies, state officials, or private vendors, are fundamentally false and serve only to undermine the rule of law.

The assertion that there needs to be a "shift" toward enforceable mandates is a deliberate misrepresentation of reality. The mandates already exist. **EO 13800** explicitly requires adherence to the **NIST CSF** for all critical infrastructure sectors, and election systems were formally designated as part of this critical infrastructure in 2017. These standards are enforceable by federal law, and any noncompliance constitutes a violation of the legal obligations entrusted to election officials and their supporting agencies.

Despite this clarity, certain state officials, advisory bodies like **CISA**, and organizations such as the **EAC** have perpetuated the myth that election systems are exempt from these requirements. They have instead promoted frameworks of voluntary compliance and advisory recommendations, which are legally inadequate in the face of the binding federal standards. These actions have not only allowed systemic vulnerabilities to persist but have also created a false narrative that undermines public trust and enables willful negligence at all levels of election management.

Moreover, any contracts, legislation, or administrative actions that attempt to circumvent **EO 13800** and the **NIST CSF** are inherently null and void from their inception. **The Supremacy Clause of the U.S. Constitution** ensures that federal law takes precedence over conflicting state or local regulations. Judicial precedent, including landmark cases like ***Marbury v. Madison***, affirms that laws repugnant to the Constitution are void and

impose no obligation on the people. This principle extends to federal cybersecurity mandates, which are designed to safeguard the nation's critical infrastructure against threats to its security and sovereignty.

The systemic noncompliance with **EO 13800** and the **NIST CSF** cannot be dismissed as oversight or ignorance. It reflects a coordinated effort to subvert national security laws under the guise of protecting proprietary information, adhering to state-level legislation, or following voluntary guidelines. These justifications fail under scrutiny and reveal a pattern of deliberate defiance against the legal and constitutional standards meant to protect the American people.

In conclusion, election officials and supporting entities must comply with **EO 13800** and the **NIST CSF**. Their obligations are clear, and no amount of misdirection or legislative manipulation can override these federal mandates. Any actions or policies that contradict these standards are void, and those responsible for their creation or enforcement should be held accountable for undermining national security and the integrity of the democratic process. We, the people, are not bound to follow unlawful regulations, and no court or judge is bound to uphold them. Transparency, accountability, and adherence to the law are not optional—they are essential to preserving the trust and sovereignty of the United States.

How do election officials prevent unauthorized access to voter data?

The claim that election officials effectively prevent unauthorized access to voter data is presented as a fundamental assurance of election security. However, evidence and findings from this investigation reveal significant vulnerabilities in the systems and practices designed to protect voter data. These vulnerabilities arise not only from technical deficiencies but also from systemic failures to adhere to the federally mandated cybersecurity standards under **EO 13800** and the **NIST Cybersecurity Framework.**

Voter registration databases are a critical component of election infrastructure and are inherently vulnerable due to their reliance on interconnected systems. Despite assurances from election officials, these databases are often accessed and updated through networked environments, creating potential entry points for unauthorized actors. The integrity of these systems is further compromised by the lack of independent third-party audits to verify their security, a requirement explicitly outlined in the **NIST CSF.**

The use of cloud-based solutions, such as **Microsoft Azure**, to store and manage voter data introduces additional risks. These systems, while marketed as secure, centralize sensitive data in a manner that makes them attractive targets for cyberattacks. Without rigorous compliance with the **NIST CSF**, including measures for data encryption, access controls, and regular vulnerability assessments, the security of voter data stored in these systems cannot be guaranteed.

Another critical vulnerability is the reliance on proprietary software provided by third-party vendors such as **Dominion Voting Systems, ES&S**, and **Hart InterCivic**. These vendors often operate under confidentiality agreements that shield their software from public scrutiny, citing proprietary concerns under the **Trade Secrets Act.** However, as established, **EO 13800** and the **NIST CSF** mandate transparency and accountability for critical infrastructure, superseding any claims of proprietary privilege. The lack of transparency in these systems not only undermines public trust but also leaves voter data susceptible to exploitation.

Physical security measures, such as securing server rooms and limiting access to authorized personnel, are often highlighted as key strategies for preventing unauthorized access. While these measures are necessary, they are insufficient without robust cybersecurity protocols. For instance, the use of removable media to transfer data between systems poses a significant risk if proper scanning and security checks are not enforced. The reliance on physical measures alone creates a false sense of security that fails to address the multifaceted nature of cyber threats.

Moreover, the systemic refusal to release **cast vote records (CVRs)** and other election-related data under the guise of protecting voter privacy further obscures the vulnerabilities in these systems. By denying transparency, election officials prevent independent verification of the measures supposedly in place to secure voter data. This lack of accountability violates the principles of **EO 13800** and undermines public confidence in the electoral process.

CISA's role as an advisory agency exacerbates these issues. While it provides best practices and guidelines for securing voter data, its recommendations lack enforceability. This advisory framework allows states and vendors to sidestep compliance with federal mandates, perpetuating systemic risks. The absence of meaningful enforcement mechanisms undermines the effectiveness of these guidelines and leaves critical vulnerabilities unaddressed.

While election officials claim to prevent unauthorized access to voter data, the reality is that systemic vulnerabilities persist at every level of the infrastructure. These vulnerabilities stem from a lack of adherence to federally mandated cybersecurity standards, inadequate oversight of third-party vendors, and a refusal to provide transparency. The narrative of secure voter data is not supported by the evidence, and without substantial reform, these systemic issues will continue to jeopardize the integrity of U.S. elections.

What happens if there is evidence of a cyberattack on election infrastructure?

The claim made by the **National Association of Secretaries of State (NASS)** that election officials work closely with federal agencies like the **Cybersecurity and Infrastructure Security Agency (CISA)** and the **Federal Bureau of Investigation (FBI)** to respond effectively to evidence of cyberattacks on election infrastructure paints an optimistic picture. They emphasize partnerships with the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** and highlight supposed incident response protocols and resilience measures as safeguards against these threats. However, this portrayal starkly contrasts with the realities exposed by high-profile breaches like the ***SolarWinds Orion hack*** and the ***2016 Russian interference*** in U.S. elections.

In the ***SolarWinds Orion hack***, Russian state actors infiltrated the supply chains of federal agencies, private entities, and state governments, remaining undetected for months. This breach laid bare systemic flaws in cybersecurity, including delayed detection, fragmented responses, and a lack of meaningful accountability. Despite **CISA's** involvement, the response was slow and uncoordinated, leaving many affected parties to fend for themselves. This glaring lack of collaboration undermines **NASS's** narrative of seamless partnerships and coordinated responses to cyber threats. Instead of resilience, the incident revealed a fragile and fragmented system incapable of mounting a unified defense.

Similarly, the ***2016 Russian interference*** in U.S. elections exposed vulnerabilities in voter registration systems across multiple states. Despite federal agencies' knowledge of the intrusions, states displayed inconsistent levels of preparedness and response. Many were unaware of the breaches until notified by federal agencies well after the fact. Even when vulnerabilities were identified, systemic reforms to secure these systems were

absent. This failure to act comprehensively refutes **NASS's** claims of robust protocols and federal support.

Central to these failures is the glaring absence of enforceable cybersecurity standards. **NASS** claims that partnerships with **EI-ISAC** and guidance from **CISA** ensure resilience, but these are merely advisory and lack binding authority. The voluntary nature of these frameworks allows vulnerabilities to persist unaddressed. The foundational mandates of **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)**, which require transparency, accountability, and third-party audits, remain sidelined in favor of superficial risk mitigation measures. By failing to enforce these federally mandated standards, election officials and vendors leave critical infrastructure exposed to preventable cyber threats.

Another key inconsistency in **NASS's** narrative is the depiction of incident response protocols. While they assert the existence of robust measures to detect, mitigate, and recover from cyber incidents, the ***SolarWinds*** and ***2016 election interference*** cases demonstrated otherwise. In both instances, response protocols were either nonexistent or insufficiently implemented. Furthermore, the lack of independent audits and comprehensive risk assessments, as required by the **NIST CSF**, perpetuates a reactive rather than preventative approach to cybersecurity.

The claim that resilience measures such as backup systems and auditing processes ensure the security of election infrastructure is similarly undermined. The ***SolarWinds breach*** highlighted the vulnerabilities of supply chains, while the ***2016 interference*** revealed the fragility of voter registration databases. These examples underscore the systemic neglect of proactive measures to secure election systems, further exposing the inadequacy of **NASS's** asserted resilience.

In practice, these failures highlight a broader systemic issue. Federal agencies like **CISA** and advisory bodies like **NASS** and **EI-ISAC** project an illusion of preparedness and collaboration, but their lack of enforcement mechanisms and adherence to federal standards belies their rhetoric. The reliance on voluntary compliance and advisory recommendations creates an environment where vulnerabilities persist unchecked, leaving election systems vulnerable to sophisticated attacks.

The discrepancies between **NASS's** portrayal of cyberattack response and the documented failures in cases like ***SolarWinds*** and ***2016 Russian interference*** reveal systemic negligence. The refusal to align with **EO 13800** and the **NIST CSF** reflects a

deliberate avoidance of accountability, leaving the integrity of U.S. elections in jeopardy. Without enforceable standards and transparent, proactive measures, these vulnerabilities will continue to undermine both the security of elections and public trust in democratic processes.

CrowdStrike's role as a central provider of endpoint security services for election systems nationwide raises significant concerns about the integrity of U.S. election infrastructure. While marketed as a robust and reliable cybersecurity solution, **CrowdStrike's** reliance on third-party software like ***FastJSON*** and ***RapidJSON*** introduces critical vulnerabilities that have been exploited in the past by Advanced **Persistent Threat (APT)** groups, particularly those linked to **Chinese state-sponsored actors.** This dependency on flawed software frameworks poses substantial risks to the integrity of the systems **CrowdStrike** is entrusted to protect.

The **Falcon platform, CrowdStrike's** flagship security solution, is widely deployed in election centers to safeguard sensitive systems such as voter registration databases, electronic poll books, and tabulation devices. However, the platform's reliance on third-party JSON processing libraries has created exploitable vulnerabilities. Both ***FastJSON*** and ***RapidJSON***, while popular for their speed and efficiency, have documented security flaws that leave systems open to serious attacks. ***FastJSON***, for instance, has been implicated in deserialization vulnerabilities that enable attackers to execute arbitrary code and compromise entire networks. Similarly, ***RapidJSON's*** poor input validation mechanisms have made it a frequent target for injection attacks, providing a pathway for malicious actors to gain unauthorized access.

These vulnerabilities are not theoretical. **Chinese APT groups** have a long history of exploiting such software dependencies to infiltrate critical infrastructure systems. These groups have demonstrated sophisticated capabilities in supply chain attacks, targeting software libraries and frameworks that are widely used across industries. Once exploited, these vulnerabilities allow attackers to bypass endpoint security measures, establish persistent access, and ex-filtrate sensitive data, all while remaining undetected.

The implications of **CrowdStrike's** reliance on these vulnerable dependencies extend far beyond individual systems. As a primary provider of cybersecurity services to election centers, **CrowdStrike's** vulnerabilities could potentially compromise entire networks of interconnected election systems. The infiltration of a single endpoint through these dependencies could allow attackers to pivot across networks, gaining

access to voter registration data, election result reporting systems, and even the administrative controls of election infrastructure.

Moreover, **CrowdStrike's** history includes several incidents that raise questions about its reliability and transparency. Past breaches involving **CrowdStrike's** clients, combined with its use of third-party libraries with known vulnerabilities, underscore systemic issues in its approach to cybersecurity. Despite its reputation as a leading cybersecurity firm, **CrowdStrike's** reliance on flawed dependencies illustrates a broader failure to implement the rigorous standards mandated by the **NIST Cybersecurity Framework (CSF)** and **Executive Order 13800.** These federal mandates require proactive risk management, transparency, and robust mitigation strategies—standards that are undermined by the presence of such vulnerabilities in **CrowdStrike's** platform.

The risks associated with these vulnerabilities are exacerbated by the opacity surrounding the use of third-party software in election systems. State election officials and the public have limited insight into the specific technologies and dependencies used by companies like **CrowdStrike**, creating a barrier to accountability. Furthermore, the lack of independent, third-party audits of these systems leaves these vulnerabilities unaddressed, perpetuating the false narrative that election systems are secure.

CrowdStrike's prominent role in securing election infrastructure makes it a critical link in the chain of national security. However, its reliance on vulnerable software dependencies like ***FastJSON*** and ***RapidJSON***, combined with its opaque practices, undermines its claims of providing reliable protection. These vulnerabilities are not merely technical oversights but systemic failures that highlight the urgent need for transparency, accountability, and strict adherence to federal cybersecurity mandates. Without addressing these fundamental flaws, the security of U.S. election systems remains precarious, leaving them vulnerable to exploitation by foreign and domestic threats.

The response to cyberattacks on election infrastructure, as portrayed by federal agencies and organizations like **CISA, EAC**, and **CrowdStrike**, paints a dismal picture of accountability and efficacy. Despite the wealth of guidance, voluntary standards, and advisories, the reality is starkly different when covert, sophisticated cyber threats emerge. The ***SolarWinds Orion hack*** and the ***2016 Russian interference*** in voter registration databases illustrate the persistent vulnerabilities in critical infrastructure and the failure of the current framework to adequately address them. More troubling, these

failures are compounded by the continued reliance on vulnerable third-party software, such as ***FastJSON*** and ***RapidJSON***, which **CrowdStrike** employs even now.

In the case of ***SolarWinds Orion***, the breach went undetected for months, allowing malicious actors to infiltrate government agencies, private corporations, and election-related infrastructure. Similarly, the ***2016 interference*** by **Russian actors** demonstrated how vulnerabilities in voter registration systems could be exploited to sow distrust and chaos in the electoral process. These incidents highlight a critical flaw: the inability of existing security frameworks to detect, mitigate, and respond to covert, weaponized malware in a timely and effective manner. Worse yet, in many instances, these breaches are discovered long after the damage has been done—if they are discovered at all.

CrowdStrike, touted as a leader in endpoint security, exemplifies the systemic issues that perpetuate these risks. Its continued use of third-party software like ***FastJSON*** and ***RapidJSON***, both with known vulnerabilities exploited historically by **Chinese APT groups**, introduces attack vectors into election systems across the nation. These dependencies create opportunities for persistent, covert infiltration, where malware can remain undetected, capable of executing attacks at the attackers' discretion. This mirrors the pattern seen in the ***2015 Office of Personnel Management (OPM) breach***, where **Chinese actors** compromised sensitive data on millions of federal employees—a breach so comprehensive and covert that it became a global lesson in cybersecurity failures.

The responses to these breaches highlight systemic complacency. Despite the severity of these incidents, there has been no meaningful accountability. **CrowdStrike** continues to operate as a trusted provider in securing election systems, even as its practices and dependencies remain unchanged. Federal agencies, tasked with protecting critical infrastructure, have failed to enforce standards that could mitigate these risks. The **Department of Justice (DOJ)**, while technically empowered to prosecute violations of federal cybersecurity mandates under **EO 13800** and the **NIST CSF**, has taken no significant actions to address these systemic failures. Instead, the narrative of voluntary compliance persists, leaving vulnerabilities unaddressed and the perpetrators of these attacks unpunished.

The reliance on voluntary standards and guidance from advisory agencies like **CISA** and the **EAC** perpetuates a false sense of security. These organizations claim to provide best practices and recommendations, but their frameworks lack enforceability and fail to align with the strict requirements of **EO 13800** and the **NIST CSF**. The result is a

patchwork system where states and vendors are left to self-regulate, often prioritizing proprietary concerns over transparency, security, and accountability. This approach not only fails to deter sophisticated adversaries but actively enables the proliferation of systemic vulnerabilities.

Ultimately, the current paradigm leaves election systems and the broader national security landscape dangerously exposed. The failure to detect and respond to covert cyberattacks, the lack of accountability for breaches, and the ongoing reliance on flawed practices and dependencies collectively create a ***clear and present danger*** to the ***United States of America.*** This threat is not theoretical; it is real, persistent, and growing. Without immediate adherence to federally mandated cybersecurity standards, the integrity of U.S. elections and the security of the nation's critical infrastructure will remain at the mercy of both foreign adversaries and domestic negligence.

#TrustedInfo2024 _ NASS.pdf

https://docdro.id/LlfY67g

Election FAQs - NASED.pdf

https://docdro.id/wJBO8lE

CISA Support to the Election Infrastructure Subsector

The document titled ***"CISA Support to the Election Infrastructure Subsector"*** provides an ostensibly thorough overview of the agency's involvement in election security, particularly following the 2017 designation of election infrastructure as critical infrastructure. This designation, while framed as a protective measure against foreign interference and domestic vulnerabilities, has facilitated a profound shift in the governance of state election systems, embedding federal oversight into processes historically managed by states. The document highlights **CISA's** tools and initiatives, including Albert sensors, the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**, tabletop exercises, and cloud solutions, but its language reveals a carefully crafted narrative that masks significant shortcomings, legal evasions, and structural vulnerabilities in the national election security framework.

At the core of **CISA's** approach is its partnership model, epitomized by the **EI-ISAC.** Presented as a collaborative forum to share information and mitigate risks, **EI-ISAC's**

operational model centralizes sensitive data flows under federal purview, ostensibly to enhance responsiveness to cybersecurity threats. However, this centralized control raises immediate concerns about state sovereignty and the independence of electoral processes. By embedding itself as a coordinator, **CISA** has positioned the federal government as an indispensable node in election operations, bypassing traditional jurisdictional boundaries under the guise of technical necessity.

Albert sensors are perhaps the most visible expression of this overreach. Deployed in all 50 states, these sensors monitor network traffic for anomalies, providing real-time alerts of potential intrusions. While this surveillance capability is marketed as a cornerstone of election security, it effectively grants federal authorities, including **CISA** and its partners, visibility into state election infrastructure without the safeguards of independent oversight or transparency. The absence of publicly available audits or documentation verifying the efficacy, scope, and limits of **Albert sensors** further compounds these concerns. The potential for misuse, whether through intentional overreach or unintentional vulnerabilities in the sensors themselves, cannot be dismissed given the high stakes of election integrity and the lack of clarity regarding the data's chain of custody.

The presentation touts significant engagement in vulnerability scanning and assessments, claiming over 500 instances of cyber hygiene evaluations and related services between October 2020 and September 2021. Yet, these numbers should be scrutinized in the absence of mandatory independent audits. **EO 13800**, the cornerstone executive order mandating adherence to the **NIST Cybersecurity Framework (CSF)** for critical infrastructure, emphasizes third-party assessments to ensure impartial verification of compliance. By relying on internally coordinated scans and self-reported metrics, **CISA** sidesteps this legal mandate, creating a self-referential loop of accountability that undermines public trust and security outcomes. The apparent preference for advisory roles and voluntary compliance over enforceable measures perpetuates systemic vulnerabilities, leaving critical infrastructure inadequately protected from both external threats and insider risks.

Tabletop exercises, a recurring theme in **CISA's** election security efforts, reflect a similar dynamic. These drills, conducted in partnership with state officials and private vendors, are framed as proactive measures to simulate and address potential threats. However, the scenarios presented—ransomware attacks, phishing schemes, and infrastructure disruptions—rely heavily on post-incident response rather than preemptive

compliance with established cybersecurity frameworks. This reactive posture neglects the foundational need for robust, verifiable security practices, such as rigorous patch management, comprehensive risk assessments, and independent validation of system integrity. Moreover, the participation of private vendors, including those with a documented history of vulnerabilities, highlights a troubling reliance on proprietary systems and third-party software that remain shielded from scrutiny under the misapplication of the **Trade Secrets Act.**

The reliance on cloud solutions, particularly **Microsoft Azure**, further exemplifies the structural risks embedded in **CISA's** approach. While cloud platforms are promoted for their scalability and resilience, their integration into election infrastructure introduces significant risks tied to centralization. Centralized data repositories create single points of failure and amplify the consequences of breaches, a reality underscored by the persistent vulnerabilities associated with cloud-based systems. Despite these well-documented risks, the document provides no substantive discussion of mitigation strategies or accountability frameworks for vendors who fail to meet security expectations. This omission aligns with a broader pattern of prioritizing convenience and centralization over decentralized resilience and transparency.

Also highlighted is **CISA's** regional offices and the role of **EI-ISAC** as critical nodes in its operational network. While these entities are presented as extensions of federal support, their structure effectively consolidates influence, eroding the autonomy of state election officials. By embedding these layers of coordination, **CISA** transforms its advisory mandate into de facto control, using the pretext of partnership to enforce conformity with its frameworks. This dynamic not only undermines state sovereignty but also creates an environment where dissenting perspectives are marginalized under the pressure to align with federally endorsed best practices.

Particularly troubling is its failure to address the constitutional and legal implications of these practices. The ***Supremacy Clause*** and foundational rulings like ***Marbury v. Madison*** establish that state actions conflicting with federal law, including **EO 13800**, are void. Yet **CISA's** operational model relies on voluntary compliance and advisory roles, effectively bypassing the enforcement mechanisms necessary to uphold these legal standards. This deliberate evasion of binding cybersecurity mandates, coupled with the systemic lack of transparency, raises serious questions about the legality and legitimacy of **CISA's** role in election security.

The broader implications of this document extend beyond election security to the integrity of democratic governance. By framing its operations as protective measures, **CISA** obfuscates the extent to which it has centralized control over election infrastructure. This consolidation of power, presented under the guise of collaboration, represents a fundamental departure from the decentralized election system envisioned by the Constitution. The resulting framework prioritizes control over transparency, convenience over compliance, and narrative over substance, leaving critical infrastructure vulnerable and public confidence eroded.

Illustrated herein is how federal advisory agencies have institutionalized practices that undermine transparency, accountability, and legal compliance. By examining **CISA's** role through this lens, the systemic risks and deliberate evasions embedded in its operations become unmistakably clear, underscoring the urgent need for a reassessment of federal involvement in state election systems.

It also provides a detailed look at **King County, Washington**, as a microcosm of how federal oversight and **CISA's** initiatives manifest within state and local election systems. Framed as a recipient of support from the **Cybersecurity and Infrastructure Security Agency**, **King County** is presented as a model of collaboration and proactive security. Yet, beneath this narrative lies a complex dynamic where local autonomy is systematically eroded under the guise of federal partnership.

In **King County**, **CISA's** involvement is prominently reflected in the deployment of **Albert sensors**, vulnerability scanning, and participation in the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**. These tools are touted as integral to securing election infrastructure, yet their implementation creates significant concerns. The **Albert sensors**, for instance, provide federal entities with real-time access to network traffic originating from **King County.** This level of monitoring, while marketed as a security enhancement, grants federal authorities unprecedented visibility into local systems without sufficient safeguards or transparency. It effectively integrates **King County's** election processes into a federally managed infrastructure, raising profound questions about data control and accountability.

King County's participation in **CISA**-coordinated activities, such as tabletop exercises and incident response drills, is highlighted as evidence of robust federal-state collaboration. These exercises, while ostensibly aimed at strengthening preparedness, also serve to institutionalize reliance on federal guidance. This reliance diminishes the

ability of **King County** election officials to operate independently or to tailor their practices to local needs, instead aligning them with federal priorities that may not reflect the specific challenges faced by the county.

A notable aspect of **King County's** election infrastructure is its use of cloud-based solutions, including **Microsoft Azure.** While cloud platforms are celebrated for their scalability and convenience, they also introduce substantial risks tied to centralization. In combination with **Albert sensors**, these platforms concentrate sensitive voter data within systems that are not under exclusive local control. The document fails to address how such vulnerabilities are mitigated, nor does it clarify the obligations or accountability of the private vendors managing these platforms. This lack of transparency raises critical concerns about data security and the potential for exploitation.

The **EI-ISAC** framework further illustrates the consolidation of control under federal auspices. By participating in this information-sharing network, **King County** integrates its election systems into a structure directed by **CISA**. While this integration is presented as a tool for enhancing security, it simultaneously restricts local officials' ability to act autonomously or to deviate from federally endorsed practices. This dynamic underscores the tension between the stated goals of collaboration and the practical reality of centralized oversight.

Crucially, the document makes no mention of independent audits or third-party assessments of **King County's** election systems, despite the clear mandates established by **Executive Order 13800**. Without such measures, the security of **King County's** infrastructure rests on self-reported metrics and internal evaluations, creating a closed loop of accountability that undermines public trust. The absence of enforceable compliance mechanisms leaves the county vulnerable to systemic risks that remain unaddressed within **CISA's** operational model.

King County's experience, as outlined in the document, exemplifies the broader themes explored in this investigation. The tools and frameworks introduced by **CISA**, while ostensibly designed to enhance security, fundamentally reconfigure the relationship between federal and local entities. Under the pretext of support, **CISA** consolidates influence over election systems, diminishing the autonomy of state and local officials while evading the accountability mechanisms required by federal cybersecurity standards.

The relationship between **King County**, **CISA**, and the federal election security framework underscores a broader strategy of integrating state and local systems into a centralized model managed at the federal level. This dynamic is not incidental but is the result of deliberate policy shifts following the 2017 designation of election infrastructure as critical infrastructure. For **King County**, this designation brought increased federal involvement, framed as support, but it has also led to a reliance on federally mandated tools and frameworks that fundamentally alter the county's operational autonomy.

Albert sensors, a hallmark of this integration, are deployed under the **EI-ISAC** framework to monitor **King County's** network traffic for potential threats. These sensors operate under the guise of improving cybersecurity but represent a direct conduit for federal oversight. Data from these sensors is shared with **CISA** and other federal entities, creating a centralized repository of election infrastructure intelligence. While this may provide real-time insights into network anomalies, it also raises significant privacy and sovereignty concerns. **King County's** election officials are effectively participants in a federally managed system, with limited transparency about how their data is used, stored, or analyzed. The absence of independent audits on the performance and security of these sensors further exacerbates these concerns, leaving **King County** without a clear mechanism to ensure accountability.

EI-ISAC, as the coordinating body for election infrastructure information sharing, acts as the nexus for integrating **King County** into a nationwide network. While information sharing is presented as a collaborative effort to enhance security, the centralized structure of **EI-ISAC** means that **King County's** role is largely that of a contributor rather than an equal partner. Data and threat intelligence flow upward to federal entities, but the reciprocal flow of actionable intelligence and resources tailored to **King County's** specific needs is less clear. This one-way dynamic effectively diminishes the county's capacity to independently address threats, instead funneling decision-making power toward federally aligned entities.

The integration of cloud solutions into **King County's** election systems introduces additional layers of complexity. **Microsoft Azure**, highlighted as a core platform for managing data, presents both logistical advantages and significant risks. Cloud solutions centralize election data storage, making it more accessible for operational efficiency but also creating a single point of failure. For **King County,** this reliance means that any breach, misconfiguration, or delay in patching cloud systems could compromise sensitive voter data and system integrity. The reliance on private vendors like **Microsoft,**

who operate under proprietary systems, further complicates accountability. The document does not provide transparency on vendor oversight mechanisms or contractual obligations to address vulnerabilities swiftly, leaving gaps in the public's understanding of how risks are managed.

Beyond technical considerations, the strategic positioning of **King County** within this federal framework raises fundamental questions about governance and democratic accountability. The involvement of **CISA** and **DHS** in shaping election security policies extends beyond advisory support into prescriptive mandates that dictate how local officials must operate. **King County's** participation in **CISA**-led initiatives like **tabletop exercises** and **coordinated vulnerability assessments** is framed as a partnership, but the top-down nature of these activities suggests otherwise. By embedding itself as an indispensable partner, the federal government effectively positions itself as a de facto manager of **King County's** election security processes, relegating local election officials to implementers of federally designed protocols.

This dynamic also has implications for public trust. **King County's** voters, like those elsewhere, are largely unaware of the extent to which federal entities influence local election systems. The opacity surrounding the integration of tools like **Albert sensors,** cloud platforms, and **EI-ISAC** into the county's operations undermines the transparency necessary for democratic accountability. Voters are left with assurances of security but little substantive evidence of compliance with federal cybersecurity standards such as those outlined in **EO 13800**. Without independent verification and public disclosure of these systems' security and efficacy, the public's confidence in the integrity of their elections remains vulnerable.

King County's reliance on federal frameworks also highlights broader systemic risks. Centralization of election infrastructure under entities like **CISA** and **EI-ISAC** creates a homogenous security posture across jurisdictions, potentially amplifying the impact of a single vulnerability. If a flaw exists within a centralized system like **Albert sensors** or Azure cloud solutions, the repercussions could extend far beyond **King County**, affecting elections nationwide. This interconnectedness, while intended to bolster security through standardization, paradoxically increases the potential for widespread disruption.

Ultimately, **King County's** relationship with **CISA** and the federal election security framework exemplifies the broader tensions explored throughout **Volume 4.** The

intersection of federal oversight, private vendor reliance, and centralized data management transforms local election systems into nodes within a nationalized infrastructure. This shift prioritizes federal control and operational convenience over local autonomy, resilience, and transparency. For **King County**, the implications are profound, as its election systems become increasingly entangled in a framework that, while claiming to enhance security, introduces new vulnerabilities and challenges to democratic accountability.

This case study reinforces the urgent need to critically reassess the role of federal entities like **CISA** in state-administered elections. **King County's** experience illustrates how federal initiatives, though well-intentioned on the surface, have systematically redefined the relationship between state, local, and federal governments in ways that undermine the principles of decentralized governance and voter trust.

CISA Support to the Election Infrastructure Subsector - King County WA CEOC - Kuennen.pdf

https://docdro.id/i3oJ2oG

CISA Stakeholder Engagement Strategic Plan (FY 2023–2025)

The ***CISA Stakeholder Engagement Strategic Plan (FY 2023–2025)*** outlines an ambitious framework for managing relationships with ***state, local, tribal, and territorial (SLTT) governments, private sector partners, and international stakeholders***. While the document outwardly focuses on collaboration, trust, and enhanced coordination, it reveals a far more complex agenda. This strategy consolidates federal influence over critical infrastructure, including election systems, by embedding **CISA's** priorities deeply into state and local operational frameworks, effectively challenging their autonomy under the guise of partnership.

At the center of this strategy lies the ***Stakeholder Relationship Management (SRM) platform***, a tool ostensibly designed to streamline interactions and improve trust-based relationships. In reality, the ***SRM platform*** functions as a sophisticated mechanism for data collection and oversight. Through stakeholder mapping and data analysis, **CISA** gathers granular intelligence on **SLTT** operations, including insights into their

vulnerabilities, challenges, and responses. This intelligence not only informs **CISA's** approach but also enables the agency to subtly guide or even dictate stakeholder activities. By controlling the flow of information and shaping stakeholder interactions, the ***SRM platform*** centralizes decision-making power within **CISA** while maintaining the facade of collaborative governance.

CISA's regional offices, tasked with implementing this engagement strategy, further illustrate the agency's intent to unify diverse jurisdictions under a centralized directive. Positioned as the primary interface between **CISA** and local entities, these offices serve as conduits for enforcing national priorities. While they provide **SLTT governments** with access to **CISA's** tools and resources, they also embed federal objectives into local decision-making processes. This integration fosters dependency, as stakeholders must align with **CISA's** strategic goals to maintain access to critical support. Over time, this dependency erodes the ability of **SLTT governments** to operate independently, effectively subordinating their needs to the agency's broader mission.

The strategic plan's emphasis on public-private partnerships introduces additional layers of complexity and risk. These partnerships, while promoted as avenues for innovation and resilience, often involve private vendors whose operations are opaque and shielded from public scrutiny. Cloud service providers, election system manufacturers, and other technology vendors frequently operate under proprietary frameworks that prioritize commercial interests over public accountability. **CISA's** reliance on these entities shifts critical infrastructure management into the hands of private actors who are not bound by enforceable cybersecurity standards. For example, the plan fails to articulate how vendors' compliance with mandates such as the **NIST Cybersecurity Framework** is verified, leaving significant gaps in accountability.

Feedback loops, a cornerstone of **CISA's** stakeholder engagement model, are similarly problematic. The plan emphasizes the importance of stakeholder input in shaping its programs and services, yet the processes for collecting and integrating this feedback are controlled entirely within **CISA's** internal structures. Tools like the ***SRM platform*** facilitate the collection of insights, but these mechanisms lack external oversight, allowing **CISA** to shape the narrative around its effectiveness without independent validation. This self-reinforcing dynamic ensures that **CISA's** initiatives are insulated from critical scrutiny, perpetuating a cycle of internal validation that sidelines dissenting perspectives and alternative approaches.

Information sharing, a recurring theme in the strategic plan, is framed as a collaborative effort to enhance resilience. However, the structures supporting this initiative, such as the **Critical Infrastructure Partnership Advisory Council (CIPAC)** and **Information Sharing and Analysis Centers (ISACs)**, centralize control over data flows under **CISA's** direction. While these entities facilitate multidirectional information sharing, they also create systemic vulnerabilities. Centralized repositories of sensitive data are attractive targets for adversaries, and the lack of detailed safeguards for protecting privacy and civil liberties raises concerns about potential misuse. The document's silence on these issues further undermines its claims of fostering trust and transparency.

One of the plan's more striking goals is its emphasis on providing easier access to **CISA's** programs, products, and resources. This goal, while aligned with **CISA's** mission to reduce risks to critical infrastructure, entrenches the agency as a gatekeeper for essential services and tools. By positioning itself as the primary intermediary, **CISA** transforms from a supportive entity into a de facto regulator, shaping critical infrastructure governance through its frameworks and priorities. This shift in role fundamentally alters the balance of power between federal and local entities, as **SLTT governments** and private actors increasingly rely on **CISA** for operational guidance and support.

The broader implications of this strategic plan extend beyond its immediate objectives, reflecting a deliberate effort to integrate state and local systems into a nationalized framework. This integration prioritizes standardization, centralized oversight, and alignment with federal objectives, often at the expense of localized flexibility and autonomy. While presented as a means to enhance resilience, this approach fundamentally redefines the relationship between federal agencies and local stakeholders, embedding **CISA's** influence in ways that challenge the principles of decentralized governance.

In the context of election systems, the strategic plan serves as a blueprint for how federal agencies can assert control over state-administered processes. By embedding itself within **SLTT** operations and leveraging its position as a coordinator, **CISA** consolidates power under the pretext of partnership. The language of collaboration masks a broader agenda of centralization, where the agency's priorities take precedence over local needs and considerations. This dynamic not only undermines the transparency and accountability essential to democratic governance but also introduces systemic risks that jeopardize the integrity of critical infrastructure.

The strategic plan, when analyzed through this lens, exemplifies the duality of **CISA's** role: projecting trust and collaboration while consolidating federal control. The agency's tools, frameworks, and engagement strategies, though outwardly supportive, function as mechanisms of influence that reconfigure the balance of power in critical infrastructure management. These practices raise urgent questions about the erosion of local autonomy, the centralization of decision-making authority, and the broader implications for public trust in government institutions. As Volume 4 continues to explore the federalization of election systems, this strategic plan emerges as a critical document illustrating how federal agencies leverage stakeholder engagement as a tool for systemic control under the guise of partnership.

The **CISA Stakeholder Engagement Strategic Plan (FY 2023–2025)** broadly outlines its stakeholders, which include:

1. **State, Local, Tribal, and Territorial (SLTT) Governments**: These entities are primary stakeholders, given their roles in managing critical infrastructure such as elections. **CISA** emphasizes building trust-based relationships with **SLTT governments** to integrate its frameworks and resources into their operations.
2. **Private Sector Partners**: This includes companies that provide critical infrastructure services, such as cloud providers (e.g., **Microsoft Azure**), election system vendors, and other technology providers. These entities play significant roles in public-private partnerships for managing infrastructure security.
3. **Federal Government Agencies**: Other federal agencies, including **DHS, FBI**, and **DOJ**, are named as collaborative partners in sharing intelligence and responding to threats. These agencies work alongside **CISA** to shape policy and operational responses.
4. **International Stakeholders**: While not heavily emphasized in the election-specific context, international stakeholders are included in broader critical infrastructure discussions, particularly in the context of cybersecurity threats and standards.
5. **Regional Offices and Coordination Councils**: **CISA's** regional offices and bodies like the **Critical Infrastructure Partnership Advisory Council (CIPAC)** serve as intermediary stakeholders to implement strategies and coordinate between federal and local entities.

6. **Information Sharing and Analysis Centers (ISACs)**: **EI-ISAC** is specifically identified as a key stakeholder in election infrastructure. **ISACs** facilitate information sharing between government and private sectors to address risks.
7. **Critical Infrastructure Owners and Operators**: These are the organizations that manage and maintain physical and digital infrastructure in sectors such as energy, telecommunications, and elections.
8. **Academia and Research Institutions**: Though less prominent, academic institutions and think tanks are often involved in developing risk assessments, frameworks, and innovations that **CISA** leverages in its engagements.

These stakeholders are unified under **CISA's** overarching strategy to align efforts across diverse entities while embedding federal priorities into localized operations.

State, Local, Tribal, and Territorial (SLTT) Governments

The involvement of state, local, tribal, and territorial **(SLTT)** governments in **CISA's** election security framework is central to the agency's broader strategy of embedding federal influence into local systems. **SLTT** governments are portrayed in the **CISA** Stakeholder Engagement Strategic Plan as essential partners in safeguarding election infrastructure. However, the practical dynamics of this relationship reveal a dependency model that subtly shifts control away from these governments, aligning their operations with federally defined priorities.

CISA provides **SLTT** governments with access to tools like Albert sensors, vulnerability assessments, and the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**. These resources are framed as supportive measures to enhance cybersecurity, but their integration into **SLTT** election systems creates a reliance on federally controlled or influenced systems. For instance, **Albert sensors**, which monitor network traffic for anomalies, are managed by **EI-ISAC** under the oversight of the **Center for Internet Security (CIS)**, a private organization contracted by **DHS**. This setup effectively places a critical layer of local election security under federal purview, as the data gathered by these sensors flows through federally funded and monitored channels. **SLTT** governments, while nominally in control of their election processes, become dependent on these systems for threat detection and response, narrowing their operational autonomy.

The strategic plan emphasizes collaboration between **CISA's** regional offices and **SLTT** governments to implement security measures and coordinate responses to potential threats. These regional offices act as intermediaries, translating **CISA's** national objectives into local action. While this structure is designed to improve responsiveness, it also centralizes decision-making authority. **SLTT** governments are encouraged, if not compelled, to align with the protocols and frameworks established by **CISA**, particularly as access to resources and support is often contingent upon compliance with these standards. This alignment raises questions about whether **SLTT** governments retain the flexibility to address localized needs independently or whether they are constrained by the broader priorities of federal agencies.

The use of cloud services, such as **Microsoft Azure**, further illustrates this dependency. Many **SLTT** election systems, including voter roll databases and ballot image storage, are hosted on cloud platforms that are deeply integrated into **CISA's** cybersecurity ecosystem. These platforms provide scalability and advanced security features, but they also consolidate sensitive data into centralized repositories. This centralization, while ostensibly beneficial for managing cybersecurity risks, creates a situation where **SLTT** governments have limited visibility into the inner workings of these platforms. Instead, they must trust the security assurances and protocols established by the federal government and private vendors, effectively relinquishing a degree of control over their most sensitive election-related data.

The strategic emphasis on information sharing further embeds **SLTT** governments into a network that prioritizes federal oversight. Through **EI-ISAC**, election officials share data on potential threats, vulnerabilities, and incidents with a centralized body that aggregates this information for analysis and dissemination. While this process is intended to enhance collective security, it also positions **CISA** and its contractors as gatekeepers of critical intelligence. **SLTT** governments, in turn, must rely on this centralized system for insights and recommendations, reducing their ability to independently assess and respond to threats. This dynamic not only impacts their operational independence but also raises concerns about transparency and accountability in the management of shared data.

CISA's strategic use of stakeholder mapping, referenced in the plan, adds another dimension to its influence over **SLTT** governments. By mapping relationships, activities, and data flows, **CISA** gains a comprehensive understanding of how **SLTT** governments interact with their election systems, stakeholders, and broader

infrastructure. This intelligence, while useful for coordinating efforts, could also be used to identify leverage points where federal priorities can be reinforced or dissenting practices minimized. The potential for such mapping to influence election outcomes indirectly, through the allocation of resources or strategic focus, highlights the broader implications of centralizing this level of operational insight.

In essence, the role of **SLTT** governments in **CISA's** election security framework reflects a delicate balance between partnership and control. While **CISA** provides valuable tools and support, the conditions of this support often place **SLTT** governments in a subordinate position, where their autonomy is overshadowed by the need to align with federal systems and objectives. This relationship challenges the traditional decentralized nature of election administration in the United States, raising critical questions about the implications of such integration for voter privacy, election integrity, and the accountability of those managing the process. As these dynamics continue to evolve, the ability of **SLTT** governments to independently secure and manage their election systems may become increasingly constrained by the structures and priorities established by **CISA** and its federal partners.

Private Sector Partners

The role of private sector partners in **CISA's** election security framework reveals a complex relationship where public and private interests intersect, often in ways that prioritize operational efficiency and innovation over transparency and accountability. These partnerships are a cornerstone of **CISA's** strategy, as outlined in the S***takeholder Engagement Strategic Plan***, and include critical collaborations with technology companies, cybersecurity firms, and election system vendors. While these relationships are framed as necessary for enhancing resilience and addressing the technological complexities of modern election systems, they also introduce significant risks tied to privatization and the opaque nature of proprietary systems.

One of the most prominent private sector roles in election security is fulfilled by companies like **Microsoft**, which provide cloud services such as **Azure** to host critical election-related data. These platforms are central to the storage and management of voter rolls, ballot images, and other sensitive election infrastructure components. While cloud providers offer scalability and advanced security features that are beyond the capacity of many local governments, they also consolidate sensitive data into centralized repositories managed by private entities. This consolidation creates potential single

points of failure and raises questions about the access and control these companies have over election data. Private sector vendors, operating under complex contractual arrangements, are often shielded by nondisclosure agreements and proprietary technologies, which limit public and government oversight.

Cybersecurity firms, such as **CrowdStrike** and the **Center for Internet Security (CIS)**, also play a critical role in managing the cybersecurity of election systems. CIS, through its management of the **EI-ISAC**, oversees the deployment and operation of **Albert sensors**, which monitor network traffic for potential threats. These sensors, funded by **DHS**, provide real-time data on election system activity, which is shared with **EI-ISAC** for analysis. The involvement of **CrowdStrike** and similar firms introduces another layer of private sector control, as these companies often provide proprietary threat detection tools and advisory services. While these firms claim to enhance election security, their reliance on proprietary software and data handling practices limits transparency. For instance, vulnerabilities in tools such as **CrowdStrike's Falcon** platform have been documented in other contexts, yet the oversight mechanisms ensuring these tools' integrity in election security remain unclear.

The plan's emphasis on public-private collaboration also highlights the integration of election technology vendors, such as those providing electronic voting machines and ballot tabulation systems. These companies are entrusted with designing and maintaining the hardware and software that underpin modern election processes. However, their operations are often opaque, with limited external auditing or compliance enforcement. The use of proprietary software in voting machines and tabulation systems further complicates oversight, as public officials and independent auditors are frequently restricted from examining the source code or system configurations. This opacity, coupled with documented vulnerabilities in some voting systems, raises concerns about the security and reliability of privately managed election technology.

CISA's reliance on private sector partners is further evident in its information-sharing frameworks. Entities like **EI-ISAC** serve as conduits for disseminating intelligence and best practices between government and private stakeholders. However, the centralized nature of these information-sharing networks creates asymmetries in access and control. Private firms, particularly those contracted to manage critical infrastructure components, often have privileged access to data and intelligence that is not equally available to the public or even to some government entities. This dynamic amplifies the influence of

private sector partners over the election security landscape, while simultaneously reducing transparency and public accountability.

The potential for conflicts of interest is another significant concern. Many private sector partners operate in a commercial context where profit motives may conflict with the public interest. For example, cybersecurity firms and technology providers have a vested interest in promoting their proprietary solutions, which may not always align with the best practices for transparency or long-term security. The lack of robust, enforceable standards for auditing and compliance further exacerbates this issue, as private firms often self-certify their systems rather than undergoing independent third-party evaluations. This reliance on self-regulation undermines the public's ability to trust the integrity of election systems.

The integration of private sector partners into election infrastructure also raises broader questions about the implications for democratic accountability. By outsourcing critical components of election security to private entities, public officials relinquish a degree of control over these systems. This shift not only complicates oversight but also creates dependencies that are difficult to reverse. If a private firm fails to meet its contractual obligations or if its systems are compromised, the repercussions could extend far beyond a single election cycle, potentially undermining public confidence in the electoral process.

The relationship between **CISA** and its private sector partners exemplifies the broader challenges of balancing innovation with accountability in the management of critical infrastructure. While private entities bring valuable expertise and resources to the table, their involvement often comes at the cost of reduced transparency and increased complexity in oversight. The reliance on proprietary systems, coupled with the lack of enforceable compliance standards, creates systemic vulnerabilities that are difficult to address within the current framework.

The role of private sector partners in election security underscores the need for greater transparency and accountability. These partnerships, while essential in many respects, also highlight the risks of centralizing control over critical election infrastructure in the hands of private entities with limited public oversight. As **CISA** continues to position itself as a coordinator of election security, the influence and practices of its private sector partners warrant closer examination to ensure that the integrity of election systems is not compromised by commercial interests or insufficient oversight.

Federal Government Agencies

The involvement of federal government agencies in **CISA's** election security framework reflects a strategic alignment aimed at centralizing oversight of critical infrastructure while presenting this centralization as a necessary response to cybersecurity threats and foreign interference. Agencies like the **Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI)**, and **Department of Justice (DOJ)** are key collaborators with **CISA** in this effort, each playing distinct roles that collectively amplify federal influence over state-administered elections.

The **Department of Homeland Security,** as **CISA's** parent agency, provides the overarching structure and funding for many of **CISA's** initiatives. Following the 2017 designation of election infrastructure as critical infrastructure, **DHS** assumed a central role in coordinating the federal government's involvement in securing election systems. This designation, while ostensibly protective, positioned election systems within the broader national security apparatus, effectively granting **DHS** and its sub-agencies a mandate to oversee and influence election security measures. This relationship empowers **CISA** to act as a conduit for federal priorities, embedding **DHS's** strategic objectives into state and local election systems.

The **FBI's** role within this framework focuses on intelligence gathering and threat response. Through partnerships with **CISA** and **EI-ISAC**, the **FBI** contributes to the identification and mitigation of cybersecurity threats to election infrastructure. **FBI Election Crime Coordinators,** for example, work directly with local election officials to investigate allegations of voter fraud, cyberattacks, and other election-related crimes. While this cooperation is essential for addressing specific incidents, it also establishes channels through which federal agencies can access sensitive election data. The coordination between the **FBI** and **CISA** underscores a broader federal strategy to integrate intelligence and operational capabilities into election oversight, raising questions about the scope and transparency of this involvement.

The **Department of Justice** complements these efforts by providing legal frameworks and prosecutorial support for election security initiatives. ***The DOJ's Election Threats Task Force, launched in response to growing concerns about threats against election officials, works closely with CISA and the FBI to ensure the security of election personnel and infrastructure. While this collaboration is framed as a protective measure, it also situates the DOJ as a critical enforcer of federal policies related to***

election security. This enforcement role, coupled with the DOJ's ability to interpret and apply laws governing election systems, positions the agency as a significant arbiter in disputes over election integrity and administration.

The integration of federal agencies into **CISA's** election security framework extends beyond operational support to include information sharing and policy development. Structures like the **Election Infrastructure Subsector Government Coordinating Council (GCC)** serve as platforms for federal agencies to collaborate with state and local officials. These councils, while promoting coordination, also centralize decision-making processes, as federal entities often set the agenda and priorities for election security initiatives. This dynamic effectively aligns state and local actions with federal objectives, further consolidating control over election systems.

A critical element of this federal involvement is the flow of intelligence and data between agencies. **CISA's** partnership with **EI-ISAC** facilitates the aggregation and analysis of cybersecurity data from across the country, which is then shared with federal entities like **DHS** and the **FBI**. This centralized data collection, while valuable for identifying national trends and threats, creates potential vulnerabilities in terms of privacy and misuse. The lack of transparency regarding how this data is managed, who has access, and for what purposes it is used raises significant concerns about the potential for federal overreach.

The reliance on federal funding for many of these initiatives further ties state and local governments to the priorities of agencies like **DHS** and **CISA**. Federal grants, such as those provided through the ***Homeland Security Grant Program***, often come with conditions that require adherence to federally defined cybersecurity frameworks and participation in **CISA-**led programs. While this funding is critical for resource-constrained jurisdictions, it also serves as a mechanism for embedding federal oversight into state and local election systems. This dynamic shifts the balance of power, making state and local governments reliant on federal resources and, by extension, federal approval for their election security measures.

The presence of federal agencies in **CISA's** election security ecosystem also raises questions about the implications for democratic accountability. By centralizing oversight within a national framework, the federal government assumes a level of control over election systems that traditionally operated under state and local jurisdiction. This centralization, while justified by the need to address cybersecurity threats, creates

tensions between the principles of state sovereignty and the realities of modern election security. The potential for these agencies to influence election outcomes, whether through direct action or the shaping of policies and practices, underscores the need for greater transparency and accountability.

The role of federal government agencies in election security highlights the interplay between national security and democratic governance. Agencies like **DHS**, **FBI**, and **DOJ** bring critical resources and expertise to the table, but their involvement also reflects a broader federal strategy to centralize control over election systems under the pretext of collaboration and protection. This dual role—as both protectors and overseers—raises fundamental questions about the balance of power in the U.S. electoral system and the implications for state and local autonomy. As **CISA** continues to expand its influence, the roles and actions of these federal agencies warrant close scrutiny to ensure that their involvement enhances, rather than undermines, the integrity and transparency of the electoral process.

The **Department of Justice's** involvement in election security, particularly through its ***Election Threats Task Force***, places it in a pivotal position as both an enforcer of federal policy and a safeguard against threats to election personnel and infrastructure. However, when analyzed through the lens of compliance with **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)**, the **DOJ's** actions—or lack thereof—raise profound concerns about complicity in systemic failures to uphold national security mandates.

EO 13800 explicitly requires adherence to the **NIST CSF** for critical infrastructure, including election systems. As one of the federal agencies most closely tied to the enforcement of laws and policies affecting election integrity, the **DOJ** cannot claim ignorance of this foundational executive order. Its failure to address the lack of compliance with **EO 13800** across state and local election systems points directly to willful negligence. The **DOJ's** responsibility goes beyond mere awareness; it has a duty to ensure that all entities under its purview, including those it collaborates with through initiatives like the ***Election Threats Task Force,*** are operating in compliance with these mandates. The absence of any **DOJ**-driven enforcement or public acknowledgment of this non-compliance indicates a deliberate choice to ignore these critical requirements.

The **DOJ's** collaboration with local election officials, auditors, and agencies such as **CISA** and the **FBI** further underscores the depth of its involvement. Evidence of **DOJ**

meetings with county-level auditors to instruct them on reporting “threats” highlights its active engagement in shaping election security practices at the ground level. This direct involvement eliminates any plausible deniability regarding the **DOJ’s** awareness of the systemic issues within the election infrastructure. The agency’s silence on the failure to meet the standards outlined in **EO 13800** and the **NIST CSF** suggests complicity, as it knowingly allows these lapses to persist without intervention or corrective action.

This complicity is compounded by the **DOJ’s** role as a legal authority. As the federal government’s primary enforcer of laws, the **DOJ** has a unique obligation to address violations of national security mandates. Its failure to act on the systemic disregard for **EO 13800** translates to tacit approval of these violations. Ignorance of the law is not a defense, particularly for an agency charged with upholding the legal framework of the nation. This standard applies even more stringently to the **DOJ**, given its access to legal expertise, intelligence, and executive directives. By not addressing these failures, the **DOJ** has positioned itself not as a protector of election integrity but as a participant in a broader pattern of negligence that jeopardizes national security.

The implications of this willful negligence are profound. Intent can be inferred from the **DOJ’s** continued inaction despite its clear awareness of these issues through its partnerships and meetings with election officials. Intentional disregard for **EO 13800** and the **NIST CSF**, coupled with the **DOJ’s** active role in shaping election security policies, aligns its actions—or lack thereof—with aiding and abetting systemic vulnerabilities. These vulnerabilities are not merely theoretical; they represent exploitable gaps in the nation’s critical infrastructure that could be leveraged by foreign or domestic adversaries. By enabling these gaps to persist, the **DOJ** becomes complicit in undermining the very systems it claims to protect.

The translation of this complicity into aiding and abetting adversaries elevates the **DOJ’s** actions to a level of treason. The agency’s failure to enforce compliance with national security directives effectively undermines the constitutional foundations of decentralized election administration and the integrity of democratic processes. Whether through active neglect or deliberate intent, the **DOJ’s** actions—or lack thereof—serve to weaken the nation’s defenses against both internal and external threats.

This analysis places the **DOJ** at the center of a systemic failure to uphold the rule of law in election security. Its role as a legal authority and its close collaboration with state and local election officials render it uniquely positioned to address these failures. Instead, its

inaction reveals a pattern of willful negligence that translates to intentional subversion of national security mandates. These actions have far-reaching implications, not only for the integrity of election systems but also for the accountability of one of the highest branches of the federal government. The **DOJ's** actions must be examined as part of a broader narrative of systemic failure and deliberate neglect, raising critical questions about the integrity and accountability of the federal agencies charged with safeguarding the nation's most fundamental democratic processes. ***This is a CLEAR AND PRESENT DANGER to the national security of the United States.***

International Stakeholders

International stakeholders, as described in the **CISA** ***Stakeholder Engagement Strategic Plan***, occupy a nuanced position in the broader framework of election infrastructure security. While not as prominently featured as domestic partners, their inclusion signals the global dimensions of cybersecurity and critical infrastructure management. These stakeholders primarily include **allied governments, multinational organizations,** and **international private entities** that contribute expertise, threat intelligence, and technological solutions. However, their involvement also introduces complexities that merit closer scrutiny, particularly when examined in the context of election systems and national sovereignty.

CISA's engagement with international stakeholders is often framed as a collaborative effort to address global cybersecurity challenges. By sharing intelligence and best practices with allied nations, **CISA** positions itself as a leader in fostering a unified approach to securing critical infrastructure. For instance, partnerships with entities like the ***Five Eyes intelligence alliance*** allow for the pooling of resources and intelligence to combat transnational cyber threats. In theory, this collaboration enhances the security of election infrastructure by providing insights into emerging threats and access to advanced cybersecurity tools developed overseas.

However, the integration of international stakeholders into election security also presents significant risks. First and foremost is the issue of data sharing. As part of its information-sharing initiatives, **CISA** relies on platforms and agreements that facilitate ***the exchange of sensitive data between the U.S. and its allies***. This data often includes ***cybersecurity threat intelligence,*** but there is potential for overlap with ***election-related information***, particularly if these systems are interconnected or share the same ***monitoring and analytics infrastructure.*** The lack of transparency surrounding what

data is shared, with whom, and under what conditions raises concerns about the exposure of sensitive election systems to foreign entities.

Another critical concern is the reliance on international private sector companies for key components of election infrastructure. **Multinational corporations** often play a central role in providing hardware, software, and cloud services for election systems. For example, if a company with international ties is contracted to manage a state's voter roll database or provide cloud hosting for ballot images, the potential exists for foreign influence or access to these systems. Even if these companies are headquartered in allied nations, their global operations may expose election systems to vulnerabilities through supply chain risks, jurisdictional conflicts, or inadequate oversight.

International stakeholders' influence also extends to policy development. Global organizations and allied governments often contribute to the creation of cybersecurity standards and frameworks that CISA adopts or promotes. While these contributions can enhance security by incorporating diverse perspectives and expertise, they may also dilute national sovereignty over critical election systems. The adoption of international standards, particularly those shaped by private interests or foreign governments, risks creating dependencies that undermine the independence and security of U.S. election infrastructure.

Furthermore, the involvement of international stakeholders complicates the accountability framework for election security. In cases of breaches or failures, tracing responsibility becomes more challenging when **multiple international actors** are involved. This diffusion of accountability is exacerbated by the proprietary nature of many ***international private sector solutions,*** which often ***operate under layers of legal protections and intellectual property rights that limit transparency.***

The strategic use of international partnerships by **CISA** also raises questions about the potential for geopolitical considerations to influence election security measures. While alliances with allied nations are intended to bolster security, they also reflect broader foreign policy priorities. ***The alignment of election security initiatives with these priorities could introduce biases or conflicts of interest that compromise the impartiality and integrity of the systems being protected.***

Finally, there is the risk of ***adversarial infiltration***. While **CISA** emphasizes partnerships with allied nations, ***the interconnected nature of global systems and supply chains creates opportunities for adversaries to exploit these relationships***.

Whether through direct infiltration of multinational corporations, supply chain attacks, or the use of allied systems as intermediaries, the involvement of international stakeholders introduces vulnerabilities that adversaries could exploit to influence or disrupt U.S. election systems.

The role of **international stakeholders** in election security underscores the inherent tension between collaboration and control. While their contributions can enhance security by addressing transnational cyber threats, they also introduce risks tied to ***data sharing, accountability, and sovereignty***. These dynamics warrant close examination, particularly as they intersect with the broader themes of federal oversight and the ***privatization of critical election infrastructure***. As the investigation unfolds, understanding the implications of these international partnerships is essential to addressing the systemic vulnerabilities they may create.

The influence of **international stakeholders** in shaping cybersecurity policies and frameworks for U.S. election systems introduces a profound and systemic vulnerability that undermines the integrity, sovereignty, and security of critical infrastructure. By adopting international standards and engaging with multinational corporations that operate outside the purview of U.S. federal law, agencies like **CISA**, the **DOJ**, and their counterparts are complicit in allowing adversarial risks to persist. This pattern of willful negligence—manifest in their failure to enforce compliance with **EO 13800** and the **NIST CSF**—has created an environment where foreign and private interests hold disproportionate influence over national election security.

The adoption of international standards for cybersecurity is often justified as a means to integrate best practices and foster collaboration. However, these standards are frequently shaped by entities with competing priorities, including multinational corporations and global organizations that may be driven by commercial interests rather than national security imperatives. When **CISA** and other federal agencies incorporate such standards into their frameworks, they risk embedding dependencies that compromise the independence of U.S. election infrastructure. For example, proprietary solutions developed by international private-sector entities often do not adhere to the stringent requirements of the **NIST CSF**, leaving critical systems exposed to vulnerabilities that could be exploited by adversaries.

The reliance on multinational corporations for essential components of election infrastructure exacerbates this risk. Companies providing cloud hosting, hardware,

software, and supply chain solutions often operate across multiple jurisdictions, subject to varying laws and regulatory environments. This global reach introduces significant opportunities for adversarial infiltration. Supply chain vulnerabilities, such as the introduction of compromised hardware or software during production or distribution, have already been exploited in other critical sectors and remain ***a clear and present danger to election systems.*** Despite these risks, federal agencies have not enforced compliance with **EO 13800's** mandate for comprehensive cybersecurity measures, allowing these vulnerabilities to persist unchecked.

Furthermore, the use of proprietary technologies by international private-sector entities compounds the problem. Proprietary systems often shield their inner workings from public and governmental scrutiny under the guise of intellectual property protections. This opacity makes it nearly impossible to independently verify the security of these systems or to ensure they comply with federal cybersecurity standards. By relying on these solutions, agencies like **CISA** and the **DOJ** are effectively outsourcing critical components of national security to private entities whose priorities may not align with the public interest.

The failure of federal agencies to address these vulnerabilities is not merely an oversight—it is an abdication of their responsibility to safeguard the nation's critical infrastructure. The **DOJ's** lack of enforcement of **EO 13800**, despite its awareness of these issues, is particularly egregious. As the legal authority responsible for ensuring adherence to national security mandates, the **DOJ** cannot claim ignorance of the risks posed by **international stakeholders**. Its inaction signals either complicity or willful negligence, both of which amount to a breach of its duty to protect the nation.

The global nature of these risks further complicates the accountability framework. Adversarial infiltration through **multinational corporations, global systems,** and **international supply chains** creates a diffuse threat landscape that is difficult to trace or address through traditional enforcement mechanisms. However, this complexity does not absolve federal agencies of their responsibility. Instead, it highlights the need for stronger enforcement of existing laws and a reevaluation of the reliance on international stakeholders in managing critical election infrastructure.

The evidence of international influence over U.S. election systems underscores a broader failure of leadership across the federal agencies involved in election security. Entities like the **DOJ**, **CISA**, **FBI**, and **DoD** are fully aware of the risks posed by these

global dynamics, yet they have chosen not to enforce the legal and security requirements designed to mitigate them. This failure represents not only a dereliction of duty but also a direct threat to national sovereignty and democratic integrity. By allowing **international stakeholders** to shape U.S. election security policies without holding them accountable to federal cybersecurity laws, these agencies are complicit in exposing the nation to foreign interference and systemic vulnerabilities.

This pattern of negligence and complicity demands urgent scrutiny. The involvement of **international stakeholders** in U.S. election systems, facilitated by federal agencies that fail to enforce cybersecurity mandates, represents a national security crisis. These agencies' continued reliance on **multinational corporations** and **global frameworks,** despite the clear risks, calls into question their commitment to the foundational principles of national security and democratic governance. This dynamic must be explored in detail, as it highlights the systemic failures that compromise the integrity of U.S. election systems and the broader implications for national sovereignty.

Regional Offices and Coordination Councils

The role of regional offices and coordination councils in **CISA's** framework for election security represents a critical mechanism for integrating federal priorities into state and local operations. These entities are framed in the **CISA *Stakeholder Engagement Strategic Plan*** as vital extensions of the agency's mission, tasked with implementing security measures, facilitating information sharing, and coordinating responses to threats. However, their operational dynamics reveal a deliberate strategy to centralize decision-making and align regional and local jurisdictions with federally driven objectives. This integration raises important questions about transparency, autonomy, and the broader implications of such a structure for election integrity.

CISA's regional offices function as the primary interface between the federal agency and state and local governments. These offices are charged with translating national strategies into actionable plans tailored to regional contexts. While this approach is presented as a way to enhance responsiveness and efficiency, it also embeds federal influence directly into local operations. State and local officials must navigate a system where access to federal resources and support is often contingent on compliance with the frameworks and protocols established by **CISA**. This dependency dynamic effectively shifts the locus of control from local jurisdictions to the regional offices, which act as intermediaries for federal priorities.

Coordination councils, such as the **Election Infrastructure Subsector Government Coordinating Council (GCC)** and the **Sector Coordinating Council (SCC)**, play a complementary role in aligning local and regional actions with national objectives. These councils bring together federal, state, and local representatives, along with private sector partners, to discuss policy and operational strategies for securing election infrastructure. While these forums are touted as collaborative spaces for addressing shared challenges, their structure inherently privileges federal leadership. Federal agencies, including **CISA** and **DHS**, often set the agenda and drive the priorities of these councils, ensuring that local and regional actions align with the broader federal mission.

One of the key tools employed by regional offices and coordination councils is information sharing. By centralizing the flow of intelligence and data through entities like the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC),** these bodies create a unified network for monitoring and responding to threats. However, this centralization also consolidates control over critical information, limiting the ability of state and local officials to independently assess and address vulnerabilities. The reliance on centralized data hubs managed by regional offices and councils further entrenches federal oversight, making local jurisdictions increasingly reliant on federally curated intelligence.

The operational integration of regional offices and coordination councils into election security raises significant concerns about autonomy. While these entities are framed as extensions of **CISA's** support mission, their role in shaping local actions effectively diminishes the ability of state and local governments to operate independently. Decisions regarding resource allocation, threat mitigation, and policy implementation are heavily influenced, if not outright dictated, by the federal frameworks propagated through these bodies. This dynamic challenges the principles of decentralized election administration and raises questions about the balance of power between federal and local entities.

Moreover, the involvement of private sector partners in coordination councils introduces additional complexities. These partners, often representing companies with vested commercial interests, have a seat at the table in shaping election security policies and practices. Their influence, combined with the federal leadership of these councils, creates a decision-making environment where local officials may have limited agency in determining the direction of their election security efforts. This structure not only reduces transparency but also increases the potential for conflicts of interest, as private sector priorities may not always align with the public interest.

Regional offices and coordination councils also serve as key nodes for implementing federally driven initiatives such as **vulnerability assessments**, **tabletop exercises**, and **Albert sensor** deployments. While these activities are designed to enhance preparedness and resilience, they also reinforce the centralization of control. For example, ***the deployment of Albert sensors, managed through EI-ISAC and overseen by regional offices, provides federal entities with direct access to network traffic data from local election systems. This setup, while marketed as a cybersecurity enhancement, effectively embeds federal monitoring capabilities into local jurisdictions, further reducing the independence of state and local governments.***

The reliance on regional offices and coordination councils to implement **CISA's** mission underscores a broader trend of ***federalizing election security*** under the pretense of collaboration. These entities are not merely conduits for communication and support; they are mechanisms for ensuring that local actions align with federally defined priorities. This alignment, while beneficial for achieving a cohesive national strategy, comes at the cost of local autonomy and transparency. ***State and local officials are left operating within a framework where their actions are shaped by the agendas of regional offices and coordination councils, rather than by the specific needs and priorities of their jurisdictions.***

The role of regional offices and coordination councils illustrates the ***systemic challenges posed by the federalization of election security.*** While these entities provide valuable resources and coordination, their function as extensions of federal oversight raises critical questions about the balance of power, the influence of private sector partners, and the implications for democratic accountability. As the investigation continues, it is essential to examine how these mechanisms contribute to the broader patterns of centralization and control that undermine the independence and integrity of state and local election systems.

Information Sharing and Analysis Centers (ISACs)

The role of **Information Sharing and Analysis Centers (ISACs)**, particularly the **Election Infrastructure ISAC (EI-ISAC)**, is central to **CISA's** strategy for securing critical election infrastructure. **ISACs** are designed to facilitate the sharing of cybersecurity intelligence, best practices, and coordinated responses among government entities and private sector partners. While presented as collaborative networks aimed at enhancing resilience, their integration into **CISA's** framework raises critical questions

about centralization, transparency, and the implications for local control over election systems.

EI-ISAC, managed by the **Center for Internet Security (CIS)** and funded by **DHS**, serves as the primary **ISAC** for election infrastructure. Its stated purpose is to aggregate and disseminate threat intelligence, providing election officials with actionable insights to protect their systems from cyberattacks. This centralized approach to information sharing is framed as a necessary response to the complexities of modern cybersecurity threats, yet it simultaneously consolidates control over critical election data under a federally funded and privately managed entity.

The flow of information within **EI-ISAC** is a key point of analysis. Local election officials provide network traffic data, reports of vulnerabilities, and incident information to **EI-ISAC**, which then processes this data to identify patterns and threats. In return, **EI-ISAC** disseminates aggregated intelligence and recommendations back to election officials. While this bidirectional exchange is intended to enhance security, it also creates a dynamic where local jurisdictions are dependent on **EI-ISAC** for threat detection and mitigation strategies. This dependency limits the ability of state and local governments to independently assess their vulnerabilities or develop localized responses, reinforcing a centralized model of control.

Albert sensors, a cornerstone of **EI-ISAC's** operations, exemplify the implications of this centralized structure. These sensors, deployed across election networks nationwide, monitor traffic for anomalies and feed data into **EI-ISAC's** analysis systems. While marketed as a critical cybersecurity tool, the sensors effectively create a pipeline for federal and private entities to access real-time data from local election systems. The lack of transparency regarding how this data is handled, stored, or shared raises significant concerns about voter privacy and the potential for misuse. Furthermore, the proprietary nature of **Albert sensors**, combined with their exclusive management by **EI-ISAC**, prevents independent audits or evaluations of their effectiveness and security.

The reliance on **EI-ISAC** also introduces vulnerabilities tied to its private management. **CIS**, as the organization overseeing **EI-ISAC**, operates as a non-governmental entity that contracts with **DHS** to perform its functions. This arrangement complicates accountability, as **CIS** is not subject to the same transparency and oversight requirements as federal agencies. The proprietary systems and data-handling practices

employed by **CIS** further obscure the operations of **EI-ISAC**, limiting public and governmental understanding of how election security intelligence is managed.

The influence of federal funding on **EI-ISAC's** priorities is another critical factor. As a **DHS**-funded initiative, **EI-ISAC** operates within the strategic objectives defined by federal agencies. This alignment ensures that the intelligence shared through **EI-ISAC** supports federal priorities, but it also means that local election officials are often secondary in the decision-making process. The centralization of intelligence and the alignment of **EI-ISAC** with federal goals reduce the capacity for state and local governments to assert their autonomy or address their unique challenges independently.

The concept of information sharing, while foundational to **EI-ISAC's** mission, also presents systemic risks. Centralized data repositories, such as those maintained by **EI-ISAC**, create attractive targets for adversaries. The aggregation of sensitive information from election systems across the country amplifies the potential impact of a breach, as a single point of failure could compromise data from multiple jurisdictions. Additionally, the lack of clarity regarding data-sharing agreements and the potential for intelligence to be disseminated beyond election officials to other federal or private entities further complicates the risk landscape.

The broader role of **ISACs** within **CISA's** framework reflects a deliberate strategy to centralize critical functions under federally aligned entities. While **EI-ISAC** provides valuable resources and intelligence to election officials, its operations illustrate the trade-offs of this model. The dependence on a privately managed, federally funded **ISAC** for core cybersecurity functions challenges the decentralized nature of U.S. election administration and introduces vulnerabilities tied to centralization and privatization.

The role of **ISACs**, and **EI-ISAC** in particular, highlights the systemic issues of transparency, accountability, and control within **CISA's** election security framework. By examining the operations of **EI-ISAC**, its integration with federal agencies, and its impact on state and local election systems, the broader implications of centralized information sharing for democratic governance and national sovereignty become clear. These dynamics underscore the need for a critical reassessment of the balance between collaboration and control in securing election infrastructure.

The **Multi-State Information Sharing and Analysis Center (MS-ISAC)** operates as a critical component of the national cybersecurity framework, emphasizing its mission to

serve **state, local, tribal, and territorial (SLTT)** governments. Through its integration with **CISA** and its role as a division of the **Center for Internet Security (CIS), MS-ISAC's** involvement in election infrastructure security demonstrates a broader federal strategy of embedding centralized cybersecurity operations within decentralized election systems. This positioning, however, introduces systemic vulnerabilities tied to transparency, accountability, and potential overreach.

MS-ISAC provides a range of services, including a 24/7 Security Operations Center (SOC), threat intelligence reports, incident response, and regular advisories tailored to the evolving threat landscape. Its offerings extend to resources like the **Nationwide Cybersecurity Review (NCSR)**, which assesses the cybersecurity maturity of **SLTT** entities, and membership in the ***CIS SecureSuite*** for enhanced tool access. While these services ostensibly aim to bolster election security, their reliance on centralized data collection and analysis reinforces federal control over local operations. **SLTT** governments become dependent on **MS-ISAC's** intelligence and resources, diminishing their ability to independently manage election security without navigating this federally aligned framework.

A critical dimension of **MS-ISAC's** role is its integration with **EI-ISAC**, which automatically incorporates election offices into its membership. This dual alignment allows for seamless information sharing between election-specific and general cybersecurity initiatives, but it also centralizes data flows under **CIS's** management. The use of proprietary tools and secure portals for document sharing creates a layer of opacity, limiting public understanding of how election-related data is processed, stored, and utilized. This lack of transparency becomes particularly concerning when coupled with **MS-ISAC's** emphasis on public-private partnerships, as private entities with commercial interests gain access to sensitive information under the pretense of collaboration.

The advisories and alerts disseminated by **MS-ISAC** further illustrate its role as a gatekeeper of cybersecurity intelligence. These communications often originate from federal directives, such as **DHS**-issued Binding Operational Directives, which are then interpreted and relayed by **MS-ISAC** to its members. This chain of communication ensures that federal priorities are embedded in the cybersecurity practices of **SLTT** entities, effectively aligning local actions with national strategies. However, this alignment raises questions about the autonomy of **SLTT** governments, as they are

compelled to conform to federally dictated guidelines to access critical resources and support.

Additionally, **MS-ISAC's** focus on supply chain vulnerabilities highlights another layer of complexity in its operations. Reports of compromised hardware and software components in election systems underscore the risks associated with integrating private sector solutions into public infrastructure. These vulnerabilities are exacerbated by the proprietary nature of many cybersecurity tools and systems, which often preclude independent audits or evaluations. The reliance on private vendors, coupled with **MS-ISAC's** central role in coordinating these efforts, creates a dependency model that compromises the sovereignty of local election officials.

The interplay between **MS-ISAC** and federal entities like **CISA** and **DHS** further complicates its position. As a federally funded initiative, **MS-ISAC** operates within the strategic objectives set by these agencies, aligning its actions with broader federal priorities. This dynamic reduces the capacity for localized responses to unique challenges, as **SLTT** entities must operate within the constraints of a nationally standardized framework. Moreover, the proprietary nature of **MS-ISAC's** operations, combined with its role as a federally aligned entity, limits public accountability and oversight.

In the context of election security, **MS-ISAC** exemplifies the tension between collaboration and control. While its services and resources provide critical support to **SLTT** governments, their integration into a centralized framework raises concerns about transparency, autonomy, and the potential for overreach. This dynamic is particularly significant in the broader narrative of federal involvement in election systems, where centralized control often conflicts with the principles of decentralized governance.

Analyzing the interplay between the **Multi-State Information Sharing and Analysis Center (MS-ISAC)** and the **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)** reveals a tightly integrated structure that consolidates data sharing, intelligence dissemination, and operational control under a centralized framework managed by the **Center for Internet Security (CIS)**. While each **ISAC** serves distinct purposes—**MS-ISAC** focusing broadly on **SLTT** cybersecurity and **EI-ISAC** specializing in election infrastructure—they are fundamentally interconnected in ways that amplify federal influence over state and local operations.

The structural overlap between the two **ISACs** is deliberate. **EI-ISAC** is a specialized division within the broader **MS-ISAC** ecosystem, designed to ensure that election-specific cybersecurity concerns are addressed within the broader context of **SLTT** infrastructure protection. This integration allows for seamless information sharing and resource allocation between the two entities. Election offices that participate in **EI-ISAC** automatically benefit from the broader resources of **MS-ISAC**, including its ***24/7 Security Operations Center (SOC)***, threat intelligence reports, and incident response capabilities. Conversely, cybersecurity threats identified through **MS-ISAC's** broader operations can be filtered down to **EI-ISAC** when they pertain to election infrastructure.

This symbiotic relationship reinforces the centralization of critical cybersecurity functions under **CIS**. Both **ISACs** rely on the same technological platforms, proprietary tools, and personnel to manage their operations. This integration not only creates efficiencies in threat detection and response but also consolidates control over how cybersecurity intelligence is processed, analyzed, and disseminated. The result is a system where election-specific vulnerabilities are addressed within a larger framework that aligns with federal priorities.

However, this close integration also raises significant concerns. By consolidating the operations of **MS-ISAC** and **EI-ISAC**, **CIS** effectively positions itself as the gatekeeper for all cybersecurity intelligence related to **SLTT** governments, including election offices. This centralized model limits the ability of state and local officials to independently assess their vulnerabilities or develop localized solutions. Instead, they become reliant on the intelligence and resources provided by these **ISACs**, which are inherently aligned with the strategic objectives of **CISA** and **DHS** due to their funding and oversight structures.

The relationship between these two **ISACs** also amplifies the potential risks associated with proprietary operations. **CIS's** role as the managing entity introduces layers of opacity that obscure how data is handled and shared between the **ISACs**, federal agencies, and private sector partners. The proprietary nature of the tools and systems used by both **ISACs** precludes independent audits or public scrutiny, raising questions about the accountability of these centralized operations.

Another critical concern is the potential for data aggregation across the **ISACs** to create systemic vulnerabilities. The centralized collection and analysis of cybersecurity intelligence from both general **SLTT** infrastructure and election-specific systems

increase the risks of adversarial exploitation. A breach within one **ISAC** could potentially compromise the data and operations of the other, given their integrated structures. This interconnectedness, while operationally efficient, creates a single point of failure that could have cascading effects across **SLTT** governments and election offices nationwide.

The integration of **MS-ISAC** and **EI-ISAC** also highlights the broader trend of federalizing cybersecurity under the guise of collaboration. By aligning their operations with **CISA's** strategic objectives, these **ISACs** serve as conduits for embedding federal influence into state and local systems. This alignment ensures that **SLTT** governments operate within a nationally standardized framework, but it also diminishes their ability to exercise autonomy or address unique local challenges.

The interplay between **MS-ISAC** and **EI-ISAC** reflects a centralized approach to **SLTT** cybersecurity and election infrastructure protection that prioritizes federal objectives over localized control. While this integration provides operational efficiencies and enhances the flow of intelligence, it also introduces systemic vulnerabilities, limits transparency, and reinforces a dependency model that challenges the decentralized principles of U.S. election administration. This dynamic warrants critical examination as part of the broader investigation into federal involvement in election systems, highlighting the need to balance collaboration with accountability and sovereignty.

Critical Infrastructure Owners and Operators

The role of critical infrastructure owners and operators in the election security ecosystem is foundational to the functioning of both the physical and digital systems that underpin democratic processes. These entities, encompassing both public and private sector organizations, are responsible for managing the infrastructure upon which election systems depend. Their inclusion as stakeholders in the **CISA** framework highlights the complex interplay between ownership, control, and accountability in safeguarding election integrity. However, their integration into this framework also raises significant concerns about privatization, transparency, and the broader implications for democratic governance.

Critical infrastructure owners and operators include entities that manage data centers, telecommunications networks, cloud services, and election-specific hardware and software. These organizations are integral to the operation of voter registration

databases, electronic voting machines, ballot tabulation systems, and secure communications platforms. Their contributions are framed within **CISA's** strategy as essential for enhancing the resilience and security of election systems. Yet, the reliance on these operators introduces systemic vulnerabilities tied to privatization and the increasing centralization of critical infrastructure management.

A key dynamic within this framework is the dependence of election officials on private sector operators for essential services. Companies like **Microsoft, Amazon**, and other cloud providers host voter rolls and ballot images, offering scalability and advanced security features that local governments often lack the resources to implement independently. Similarly, manufacturers of electronic voting machines and tabulation systems provide the hardware and software necessary for conducting elections. While these operators bring technical expertise and innovation to the table, their operations are frequently shielded by proprietary frameworks and intellectual property protections. This opacity limits the ability of election officials and the public to verify the security and reliability of these systems, creating a trust deficit that undermines confidence in election integrity.

Privatization also complicates accountability. Unlike public entities, private sector operators are not directly accountable to voters or subject to the same transparency requirements. Their contractual relationships with election officials often include nondisclosure agreements and other legal protections that further obscure their operations. This dynamic shifts significant control over election infrastructure into the hands of private entities, whose primary obligations are to shareholders rather than the public. The potential for conflicts of interest is heightened in this context, as private operators may prioritize commercial considerations over the broader public interest.

The integration of critical infrastructure operators into **CISA's** information-sharing frameworks further highlights the centralization of control. These operators are often active participants in **ISACs**, where they contribute data and receive intelligence related to cybersecurity threats. While this collaboration enhances situational awareness, it also positions private operators as gatekeepers of critical information. Their involvement in these frameworks amplifies their influence over the decision-making processes that shape election security policies and practices. This influence, while beneficial in addressing technical challenges, also raises questions about the balance of power between public and private entities in managing election systems.

Supply chain vulnerabilities represent another critical concern associated with critical infrastructure operators. Many of the components used in election systems are sourced from global supply chains, exposing them to risks of tampering or compromise at various stages of production and distribution. Operators tasked with managing these systems must navigate these risks, but their ability to do so is often limited by the proprietary nature of their technologies. Federal oversight through entities like **CISA** is intended to mitigate these vulnerabilities, but the reliance on voluntary compliance rather than enforceable standards leaves significant gaps in the security framework.

The operational integration of critical infrastructure operators into **CISA's** framework underscores a broader trend of outsourcing core functions of election administration to private entities. While this approach provides technical efficiencies and access to advanced capabilities, it also shifts the locus of control away from public officials and institutions. This dynamic challenges the principles of transparency and accountability that are foundational to democratic governance. The increasing reliance on private operators, combined with the lack of robust oversight mechanisms, creates systemic vulnerabilities that are difficult to address within the current framework.

The role of critical infrastructure owners and operators reveals the tensions inherent in balancing public and private responsibilities in election security. Their contributions are essential for managing the complexities of modern election systems, but their integration into federally aligned frameworks like those overseen by **CISA** raises critical questions about transparency, accountability, and the preservation of democratic principles. As the investigation continues, it is essential to examine how these dynamics shape the broader narrative of federal involvement in election systems and the implications for public trust and national sovereignty.

The critical infrastructure owners and operators referenced in the broader election security framework include both public entities and prominent private-sector companies. Their roles are deeply integrated into managing key aspects of election systems, often involving voter registration databases, voting machines, tabulation systems, and the cloud platforms used to store and process election-related data. Among the most significant operators mentioned or inferred in various contexts are **Microsoft, Amazon, Dominion Voting Systems,** and **Election Systems & Software (ES&S)**. These entities are directly tied to election security through their technologies, services, and contractual relationships with state and local governments.

Microsoft plays a significant role in election security, primarily through its **Azure** cloud platform, which is frequently used to host voter rolls, ballot images, and other sensitive election data. **Azure's** scalability and advanced security features make it attractive to state and local governments, particularly those with limited resources for maintaining robust on-premises systems. However, this reliance on **Microsoft** also centralizes election-related data within a private infrastructure that is not entirely under public control. ***Microsoft's ElectionGuard software,*** designed to enhance the security of electronic voting systems, further embeds the company into the electoral process, creating dependencies that challenge the autonomy of local election officials. These tools are proprietary, meaning their inner workings are shielded from public scrutiny, raising concerns about their reliability and compliance with federally mandated cybersecurity frameworks such as the **NIST CSF**.

Amazon, through its **AWS** cloud services, similarly hosts critical components of election infrastructure. Many states and local jurisdictions rely on **AWS** for secure data storage and processing, including backup systems for voter registration databases. Like **Azure**, **AWS** centralizes sensitive data within a private-sector framework, introducing risks associated with potential breaches, data misuse, and lack of public oversight. Amazon's role in election security extends beyond cloud hosting; its technological capabilities, combined with its partnerships with public-sector organizations, position it as a key player in the broader cybersecurity landscape.

Dominion Voting Systems and **Election Systems & Software (ES&S)** are two of the largest manufacturers of voting machines and tabulation systems in the United States. Their hardware and software are used by numerous jurisdictions to conduct elections, making them critical operators within the election security framework. **Dominion's** systems have faced scrutiny for vulnerabilities that could potentially be exploited to alter election outcomes, while **ES&S** has similarly been criticized for opaque security practices and the proprietary nature of its technologies. These companies' reliance on proprietary software creates significant challenges for transparency, as election officials and independent auditors are often restricted from fully examining the systems to ensure their integrity. Both **Dominion** and **ES&S** participate in information-sharing frameworks like **EI-ISAC**, aligning their operations with federal cybersecurity initiatives but also reinforcing centralized control over election infrastructure.

These private-sector operators tie directly into **CISA's** election security efforts through their participation in public-private partnerships and information-sharing networks. By

integrating into **ISACs**, they gain access to federal intelligence on cybersecurity threats while contributing their own data to centralized analysis systems. This relationship amplifies their influence over election security policies and practices, often at the expense of transparency and accountability. For example, both **Dominion** and **ES&S**, as major providers of election systems, play critical roles in shaping the security protocols that local jurisdictions adopt, effectively setting de facto standards for election administration.

Another critical aspect is the role of global supply chains in these operations. Components for voting machines, tabulation systems, and even cloud infrastructure hardware are often sourced from multiple countries, including nations with adversarial interests. This dependence on international supply chains introduces vulnerabilities at every stage of production and distribution. Federal oversight mechanisms, including those overseen by **CISA**, are intended to address these risks, but the lack of enforceable standards for private operators undermines the effectiveness of these efforts.

The involvement of these critical infrastructure owners and operators illustrates a significant shift in the governance of election security. By outsourcing core functions to private-sector entities, state and local governments have become increasingly reliant on organizations whose primary accountability is to shareholders rather than the public. This dynamic challenges the foundational principles of decentralized election administration and introduces systemic risks that extend beyond individual elections to the broader democratic process.

The role of these specific operators underscores the importance of examining the privatization of election security and its implications for transparency, accountability, and national sovereignty. Their integration into federally aligned frameworks like **CISA** and **ISACs** highlights the complexities and vulnerabilities inherent in modern election systems, raising urgent questions about the balance of power between public institutions and private interests in safeguarding democracy.

Academia and Research Institutions

Academia and research institutions play a nuanced role in **CISA's** election security framework, contributing technical expertise, theoretical frameworks, and workforce development while also serving as external validators of federally driven strategies. Their inclusion as stakeholders reflects an acknowledgment of the intellectual and

scientific underpinnings required to address complex cybersecurity challenges in critical infrastructure, including election systems. However, their integration into this framework also raises questions about influence, independence, and potential conflicts of interest.

Academic institutions often collaborate with **CISA** and other federal entities to develop advanced tools, algorithms, and methodologies for identifying and mitigating cybersecurity threats. Through partnerships with **federally funded research and development centers (FFRDCs)** and **university-affiliated research organizations**, these institutions provide technical solutions tailored to specific vulnerabilities in election systems. For example, academia contributes to the development of threat modeling techniques, secure software architectures, and artificial intelligence systems designed to analyze and predict emerging threats. While these contributions are invaluable, their deployment is often mediated through proprietary channels or federal oversight, limiting their direct accessibility to state and local election officials.

Research institutions also play a critical role in testing and validating election technologies. Through rigorous assessments, they evaluate the integrity of voting machines, ballot tabulation systems, and electronic poll books. However, these efforts are frequently conducted in controlled environments that may not fully replicate real-world conditions, raising concerns about the generalization of their findings. Furthermore, many research projects are funded by federal grants or private sector partnerships, which can introduce biases in favor of the entities sponsoring the research. This potential for bias complicates the perceived independence of academic evaluations, particularly when their conclusions align with the strategic objectives of **CISA** or its private-sector partners.

Another key contribution of academia is workforce development. Universities and research institutions often serve as training grounds for cybersecurity professionals, many of whom eventually join federal agencies, private-sector companies, or election offices. Programs funded by **CISA** or affiliated organizations are designed to address the talent gap in election security, equipping professionals with the skills needed to manage and protect critical infrastructure. While this pipeline is essential for building capacity, it also creates an intellectual alignment between academia and the federal agencies that fund these programs. This alignment can blur the boundaries between independent research and federally driven agendas, potentially influencing the direction of academic inquiry.

Academia also influences public discourse on election security through white papers, policy briefs, and participation in advisory councils. These contributions help shape the narratives around election vulnerabilities, best practices, and the efficacy of current systems. However, the reliance on federally aligned institutions or funding sources means that these narratives often reinforce the status quo rather than challenge it. For instance, papers produced under federally sponsored initiatives are less likely to critique the centralization of election security functions under **CISA** or the reliance on proprietary systems managed by private-sector entities.

The integration of academia into **CISA's** information-sharing frameworks highlights another dimension of their involvement. Through participation in **ISACs** or direct collaboration with federal agencies, research institutions gain access to sensitive data and intelligence that inform their studies. While this access enhances the relevance and applicability of their work, it also ties them more closely to the operational priorities of federal entities. This dynamic risks reducing academia's role as an independent watchdog, instead positioning it as an enabler of federally driven strategies.

The global nature of academia adds another layer of complexity. Universities and research institutions often collaborate with international peers, participate in global cybersecurity initiatives, and source talent from around the world. While these activities enrich the intellectual ecosystem, they also expose U.S. election systems to potential adversarial influence. Collaborative projects with foreign institutions or researchers can inadvertently introduce vulnerabilities, particularly if these partnerships involve nations with competing geopolitical interests.

Academia's involvement in election security is both indispensable and fraught with tensions. Their contributions of technical expertise, workforce development, and public policy analysis are critical for addressing the challenges of modern election systems. However, their integration into federally aligned frameworks raises concerns about independence, transparency, and the influence of funding sources. The reliance on academia to validate and reinforce the strategies of **CISA** and its partners underscores a broader pattern of aligning intellectual resources with centralized control, often at the expense of critical scrutiny.

The role of academia and research institutions highlights the importance of examining the interplay between intellectual independence and federal influence. Their contributions are essential for advancing election security, but their close ties to federal

agencies and private-sector entities necessitate a careful analysis of their impact on transparency, accountability, and the broader narrative of election integrity. As with other stakeholders, the integration of academia into this framework reflects the challenges of balancing collaboration with autonomy in safeguarding democratic processes.

CISA-Stakeholder-Engagement-Strategic-Plan2023-2025_V3_508c.pdf

https://docdro.id/UwxNG1d

The stakeholders driving **CISA's** frameworks and the very mechanisms of election security are inseparable from those responsible for conceptualizing, implementing, and perpetuating the Risk-Limiting Audit (RLA) system. This linkage between **CISA** and the architects of the RLA reveals an intricate web of entities, individuals, and agencies that have weaponized election audits—not to secure our democratic processes, but to obfuscate, deceive, and consolidate control.

CISA's partnerships are deeply entangled with the same organizations and individuals who created and promoted RLAs as the pinnacle of election integrity. But what has emerged is far from an instrument of transparency or accountability. Instead, the RLA system has been meticulously designed to neutralize genuine calls for accountability, serve as a veneer for election integrity, and safeguard a system rife with vulnerabilities. Through its implementation, the RLA has annihilated the principles of transparency, state sovereignty, and the rights of the electorate, violating not only state constitutions and federal laws but also fundamental human rights established in international treaties.

The same stakeholders who claim to champion cybersecurity—organizations like **Microsoft, Amazon, Verified Voting, Democracy Fund, VotingWorks,** and others—are complicit in designing and deploying a system that does the opposite. The RLA presupposes the integrity of ballots, ignoring the possibility of fraud or manipulation before the audit even begins. It relies on software like ARLO, which is vulnerable to remote access exploitation, to select ballots for audits, a process that has repeatedly failed to meaningfully address contested races or uncover fraudulent activity. This is not just a flaw—it is a design feature, ensuring that RLAs can be wielded as a shield to dismiss calls for genuine forensic audits.

Further compounding this betrayal, the exemption of cast vote records (CVRs) from public records—contrary to **FOIA** and the **Federal Records Act**—ensures that the public cannot verify the integrity of their elections. This deliberate destruction of transparency directly undermines the right to anonymous voting, a cornerstone of democracy enshrined in both domestic and international law. The RLA system's function as a "***fraudulent filing system"*** weaponizes data collection, enabling entities like **CISA**, **EI-ISAC**, and the **USPS** to track and profile voters based on their electoral behavior. Combined with tools like the **ERIC** system, the **NCOA** database, **MelissaData**, and **GIS mapping software**, this profiling feeds into a broader apparatus designed to manipulate and control electoral outcomes.

These same stakeholders have crafted a system that centralizes control over election audits under the guise of "***federalized security.***" State matrices sidestep compliance with **EO 13800** and the **NIST Cybersecurity Framework**, instead allowing vendors to self-assess against weaker state-specific standards. This systemic negligence or deliberate subversion ensures that known vulnerabilities remain unresolved, leaving elections exposed to cyber threats and manipulation. It is no accident that third-party dependencies riddled with flaws, exploited in attacks like **SolarWinds**, remain in use. These failures are not isolated—they are symptomatic of a broader design to erode the sovereignty of state-run elections and consolidate control in the hands of a few.

The RLA is the crown jewel of this treasonous conspiracy. It is not merely an ineffective audit—it is a carefully engineered instrument of power preservation. By ensuring that audits never uncover fraud or discrepancies, the RLA reinforces a status quo where votes can be stolen, manipulated, or miscounted without consequence. Combined with the ***ERIC system's voter roll manipulation, the NCOA database's address validation, and GIS software's redistricting capabilities***, the RLA completes a feedback loop of fraud. It provides the final veneer of legitimacy to elections that are, in reality, federalized, controlled, and weaponized against the people.

This transition reveals the true nature of the conspiracy: a coordinated effort involving **CISA**, the **DOJ**, the **EAC**, the **FBI**, **DHS**, private corporations, and a host of **NGOs** and advocacy groups. Together, they have built an infrastructure that not only enables election fraud but also protects it under layers of legal, procedural, and technological obfuscation. The RLA system, far from safeguarding democracy, has become the mechanism by which it is systematically dismantled. As we delve into the organizations and individuals responsible, it becomes clear that this is not a story of incompetence or

error—it is a deliberate, calculated betrayal of the people, their rights, and the very foundations of the republic.

Making Every Vote Count: A Practical Guide to Risk-Limiting Audits

The document ***Making Every Vote Count: A Practical Guide to Risk-Limiting Audits*** represents a critical juncture in the timeline of the Risk-Limiting Audit (RLA) system's development and implementation. It details the carefully orchestrated efforts of a convening held on January 31, 2019, at **Microsoft's Innovation Lab** in Washington, D.C., during which a collection of stakeholders spanning government, academia, nonprofit organizations, and the private sector came together to shape the future of election auditing. This convening was far more than a collaborative brainstorming session; it was a pivotal moment in solidifying the infrastructure and methodologies that would later become the backbone of the election audit systems used in the 2020 elections and beyond.

Microsoft's involvement, as host of this event, raises significant concerns given the company's overarching role in U.S. election systems. Through its ***Defending Democracy Program*** and its cloud platform **Microsoft Azure**, **Microsoft** is deeply embedded in managing voter rolls, ballot and envelope digital image storage, and precinct-level election data. The very stakeholders designing these systems at this event are connected to the infrastructure that centralizes election data within **Microsoft's** purview. With **Azure's** integration of **GIS** mapping and querying capabilities, the potential for targeting voters or analyzing patterns based on voting trends poses significant national security and ethical risks. Such involvement also introduces questions about violations of antitrust laws, as **Microsoft's** dominance in this arena consolidates control over election infrastructure.

The timing of this event, occurring after **Executive Order 13800** mandated adherence to the **NIST Cybersecurity Framework (CSF)** for critical infrastructure, underscores the complicity of these stakeholders in bypassing federal cybersecurity requirements. While the RLA system claims to promote transparency and integrity, the convening reveals a strategy that prioritized consolidation and federal alignment over compliance with standing national security directives. These stakeholders were acutely aware of the legal and constitutional standards at play, including the protections for anonymous voting

enshrined in **state constitutions, the U.S. Constitution**, and international human rights agreements such as the **International Covenant on Civil and Political Rights** and the **Universal Declaration of Human Rights**. Yet, they proceeded to construct a framework that undermined these principles.

The convening hosted by **Microsoft** was not simply an academic exercise; it was the inception of a framework that disregards fundamental rights and facilitates systemic vulnerabilities. The timeline it represents is critical for understanding how these initiatives were intentionally designed and implemented well in advance of the 2020 elections. This meeting was a think tank of stakeholders from all areas—government agencies, academia, advocacy organizations, and private industry—who were instrumental in creating, drafting, and promoting RLAs under the guise of securing elections.

The second page of the document lists five major organizations that were central to this initiative:

1. Microsoft's Defending Democracy Program
2. Verified Voting
3. Common Cause
4. The Brennan Center for Justice
5. The National Election Defense Coalition (**NEDC**)

Each of these organizations brought a unique yet interconnected role to the table, blending advocacy, policy expertise, and technical knowledge to craft a system that would later become a cornerstone of election audits.

The list of participants reveals an extensive network of individuals and organizations complicit in these efforts. Notable participants include Jennifer Morrell, who played a pivotal role in Colorado's adoption of RLAs; Dr. Philip B. Stark, whose statistical expertise provided the foundation for RLA methodologies; Mark Lindeman of Verified Voting, a key advocate for RLA tools; and representatives from the **U.S. Election Assistance Commission (EAC)**, including Jerome Lovato. These individuals collaborated closely with technologists like Dr. Ronald Rivest, who brought decades of cryptographic and mathematical expertise to the discussion, and Maurice Turner, who bridged the gap between cybersecurity and election administration.

This gathering also involved representatives from academic institutions and research centers, whose names will be explored in greater detail as we proceed. Their

contributions were not limited to theoretical frameworks; they actively shaped the policy and operational guidelines that would dictate how RLAs were integrated into state and local election systems.

This file lays bare the convergence of the entities and individuals responsible for the RLA system's creation. These participants—whether election officials, academic researchers, nonprofit advocates, or private industry technologists—form the foundation of a broader network that has systematically dismantled the rights of voters, federalized election processes, and circumvented existing legal protections. The file's timeline and content provide a comprehensive foundation for an in-depth examination of each organization and individual involved, their affiliations, and the roles they played in orchestrating and perpetuating a coordinated effort that undermines election integrity and compromises national sovereignty.

Microsoft's Defending Democracy Program

The ***Making Every Vote Count*** document underscores ***Microsoft's Defending Democracy Program*** as a central force in the development and deployment of election security initiatives, with a focus on Risk-Limiting Audits (RLAs). This convening, held on January 31, 2019, highlights the deliberate orchestration of a framework that not only embedded Microsoft's proprietary tools but also aligned a diverse network of stakeholders with a shared goal of redefining the infrastructure of election security under centralized control.

Microsoft's role in hosting this event goes beyond the provision of resources or a neutral platform for dialogue. ***The Defending Democracy Program,*** through its integration of **Azure cloud services** and advanced **GIS mapping** capabilities, positioned **Microsoft** as a key architect of election systems that centralize data and decision-making. By embedding itself at every level of election operations—managing voter rolls, digital ballot images, and audit records—**Microsoft** has effectively consolidated control over critical electoral infrastructure, leaving local election officials dependent on its tools and systems. The convening solidified this influence by bringing together stakeholders who would align policies and methodologies to fit **Microsoft's** technological framework.

The timing of this event, after the enforcement of **EO 13800** and the **NIST Cybersecurity Framework**, highlights a strategic alignment designed to circumvent

these mandates while maintaining the appearance of compliance. Stakeholders engaged in this initiative were fully aware of the existing legal and constitutional obligations, including anonymity protections for voters under both domestic and international law. Yet, their collaboration during this convening reflects a calculated effort to centralize election systems under a corporate-dominated infrastructure that subverts these principles.

This convening also reveals **Microsoft's** broader ambitions through its **Defending Democracy Program**. Its partnerships with governments, advocacy organizations, and **NGOs** position the company not just as a service provider but as a curator of election narratives. By leveraging its role in combating disinformation, **Microsoft** has assumed the power to influence public discourse, shaping what is deemed credible or harmful information. This discretionary control raises profound concerns about the potential for censorship and the manipulation of electoral narratives under the guise of protecting democracy.

The participation of entities such as the **National Association of Secretaries of State (NASS)** and the **Election Assistance Commission (EAC)** further entrenches **Microsoft's** influence in election security policy and practice. These partnerships allowed **Microsoft** to drive the adoption of RLAs and related methodologies while embedding its proprietary systems into state and local election processes. This integration represents not merely collaboration but a shift in control over election infrastructure from public institutions to private corporate frameworks.

The ***Making Every Vote Count*** document, therefore, does more than chronicle the origins of RLAs. It exposes the intricate network of stakeholders who have systematically collaborated to centralize election security under corporate control, undermining transparency and accountability in the process. ***Microsoft's Defending Democracy Program***, operating as both a convenor and driver of this strategy, exemplifies how technology companies have leveraged their resources and influence to reshape election infrastructure in ways that prioritize centralized power over democratic governance. This convening represents a critical turning point, laying the groundwork for an election system that is no longer controlled by the people but by a carefully aligned network of corporate and governmental interests.

Verified Voting

Verified Voting has positioned itself as a prominent voice in election security, advocating for transparency and accountability through the promotion of **voter-verifiable paper audit trails (VVPATs)** and Risk-Limiting Audits (RLAs). However, its actions, affiliations, and endorsements reveal a more complicated role—one that often conflicts with the ideals of transparency and accountability it publicly champions.

The organization has played a pivotal role in promoting RLAs as a mechanism for ensuring post-election verification. **Verified Voting** collaborates closely with technologists, policymakers, and election officials to implement RLAs across the United States. This includes publishing educational resources, providing technical guidance, and partnering with influential entities such as **the Brennan Center for Justice** and **Common Cause**. Through these collaborations, **Verified Voting** has successfully positioned RLAs as the gold standard for election integrity. However, a closer examination reveals critical flaws in the systems they advocate for, flaws that the organization appears either unwilling or unable to address.

One of the most glaring issues with **Verified Voting's** advocacy for RLAs is their reliance on proprietary tools like **ARLO**. This software, marketed as a solution for conducting RLAs, centralizes control and introduces vulnerabilities that undermine transparency. **ARLO's** remote access capabilities and the exemption of cast vote records (CVRs) from public disclosure render the system opaque, hindering independent verification and opening the door to potential manipulation. These characteristics directly conflict with the stated goals of transparency and accountability, raising questions about **Verified Voting's** commitment to genuine election integrity.

Additionally, **Verified Voting's** endorsement of internet-based voting systems, such as ***Democracy Live's OmniBallot platform,*** further complicates its narrative. **OmniBallot,** which operates on **Amazon Web Services (AWS)**, centralizes sensitive election data within a corporate-controlled environment, introducing significant cybersecurity risks and undermining voter anonymity. Despite these risks, **Verified Voting** has lent its credibility to such systems, aligning with corporate interests at the expense of robust election security.

The organization's timeline of advocacy for RLAs aligns with broader efforts to federalize election systems, particularly during key events like **Microsoft's** January

2019 convening. This event brought together stakeholders from academia, private industry, and advocacy groups to refine RLA methodologies and align them with national election security frameworks. **Verified Voting's** participation in this convening underscores its role in embedding proprietary systems into the electoral landscape. This alignment, however, often comes at the expense of compliance with federal cybersecurity mandates like **EO 13800** and the **NIST Cybersecurity Framework. Verified Voting's** focus on promoting RLAs has consistently prioritized their adoption over addressing these compliance gaps.

Verified Voting's public messaging adds another layer of complexity to its role in election security. Their advocacy materials frequently highlight the statistical rigor of RLAs while ignoring their foundational flaw: the assumption that all ballots being audited are legitimate. This oversight renders RLAs ineffective in detecting systemic issues, such as fraudulent ballots, compromised voter rolls, or other irregularities. By focusing solely on the end results of audits, **Verified Voting** obscures the process's inability to address these vulnerabilities, effectively gaslighting the public into believing in the efficacy of a fundamentally flawed system.

The contradictions in **Verified Voting's** role become even more apparent when examining their actions within the broader network of election security stakeholders. While publicly advocating for transparency, their partnerships and endorsements often align with efforts to centralize control over election systems. By embedding proprietary technologies like **ARLO** and supporting platforms such as **OmniBallot**, **Verified Voting** has facilitated a system that undermines voter trust, destroys anonymity, and shifts power from decentralized governance to corporate and federal oversight.

In essence, **Verified Voting** embodies a troubling duality: a public-facing commitment to election security and transparency, juxtaposed with actions that entrench centralized control and proprietary systems. Their advocacy for RLAs and internet-based voting platforms reflects this contradiction, as these systems fail to address core vulnerabilities while creating new risks. Far from reforming election security, **Verified Voting's** role in the ecosystem of election infrastructure highlights its complicity in perpetuating the systemic flaws it claims to oppose. As we continue to investigate their affiliations and the broader implications of their actions, it becomes increasingly clear that **Verified Voting** is not just a participant in election security but a key contributor to its ongoing vulnerabilities.

Verified Voting's involvement with internet-based voting systems, particularly ***Democracy Live's OmniBallot platform,*** emerges as a critical dimension of its broader role in shaping election infrastructure. While **Verified Voting** publicly advocates for transparency and election integrity, its endorsements of systems like ***OmniBallot*** expose a troubling alignment with centralized and proprietary platforms that compromise voter anonymity, transparency, and security.

OmniBallot, developed by **Democracy Live,** is marketed as an accessible and modern solution for delivering ballots to voters, particularly those overseas or with disabilities. The platform, hosted on ***Amazon Web Services (AWS)***, centralizes sensitive election data within a cloud environment controlled by a private corporation. **Verified Voting's** support for this system reflects a contradiction in its stated mission. While the organization claims to champion secure, evidence-based elections, its endorsement of internet-based voting platforms introduces vulnerabilities that are well-documented by cybersecurity experts.

One of the most significant concerns with ***OmniBallot*** is its potential to compromise voter anonymity. By integrating ballot delivery and voting processes into a centralized system, the platform creates opportunities for tracking and analyzing voter behavior. This level of data centralization stands in stark opposition to the principles of voter privacy enshrined in both U.S. constitutional protections and international human rights agreements. **Verified Voting's** alignment with ***OmniBallot*** raises questions about its commitment to these foundational principles.

In addition to privacy concerns, ***OmniBallot*** introduces significant cybersecurity risks. Internet-based voting systems are inherently vulnerable to cyberattacks, data breaches, and foreign interference. While **Democracy Live** has implemented measures to mitigate these risks, the reliance on ***AWS*** for data storage and processing creates a dependency on a private corporation whose infrastructure is not subject to the same transparency or accountability standards as public systems. **Verified Voting's** willingness to endorse such platforms reflects a prioritization of convenience and modernization over the robust, decentralized security measures necessary to safeguard election integrity.

Verified Voting's role in promoting ***OmniBallot*** extends beyond mere endorsement. The organization's participation in events and forums where ***OmniBallot*** and similar platforms were discussed demonstrates its active involvement in legitimizing these systems. This participation includes collaborations with federal agencies, advocacy

organizations, and election officials to integrate internet-based voting solutions into the broader election security framework. By positioning ***OmniBallot*** as a tool for accessibility and modernization, **Verified Voting** has contributed to the normalization of systems that introduce significant vulnerabilities into election infrastructure.

Moreover, **Verified Voting's** public messaging around ***OmniBallot*** reflects a deliberate effort to obscure these vulnerabilities. The organization often emphasizes the platform's potential to expand voter access while downplaying or ignoring the systemic risks it introduces. This selective framing aligns with a broader trend in **Verified Voting's** advocacy, where the focus on end goals—such as accessibility or statistical rigor—overshadows critical flaws in the systems they promote.

The relationship between **Verified Voting** and **Democracy Live** also underscores the broader network of private and public entities shaping U.S. election systems. This network, which includes federal agencies, state election officials, and private corporations, operates under the guise of improving election security and accessibility. However, its reliance on proprietary technologies and centralized control mechanisms undermines transparency and accountability, raising significant concerns about the integrity of the electoral process.

In conclusion, **Verified Voting's** endorsement of ***OmniBallot*** exemplifies the contradictions at the heart of its advocacy. While the organization publicly champions secure and transparent elections, its alignment with internet-based voting platforms reveals a willingness to compromise these principles in pursuit of convenience and modernization. This duality—promoting transparency while endorsing systems that undermine it—highlights the systemic flaws in **Verified Voting's** approach to election reform. As we continue to examine its partnerships and actions, it becomes increasingly clear that **Verified Voting's** role in shaping election infrastructure is not merely inconsistent but actively contributes to the vulnerabilities it claims to address.

Verified Voting's influence within federal agencies and advocacy networks reveals a coordinated effort to shape election policies and practices, with implications that go far beyond its public-facing mission of promoting secure and transparent elections. Unlike organizations that operate primarily through direct legislative lobbying, **Verified Voting** employs a more nuanced strategy: embedding itself as a trusted advisor to government agencies and leveraging its network of advocacy partners to normalize policies and technologies that centralize control over election systems. This influence operates

through close relationships with entities like the **Election Assistance Commission (EAC), the Department of Homeland Security (DHS),** and its subsidiary, **the Cybersecurity and Infrastructure Security Agency (CISA).**

At the federal level, **Verified Voting's** technical expertise and public credibility allow it to position itself as a critical resource for shaping election security guidance. It works with the **EAC** to develop best practices and frameworks for election audits, aligning these recommendations with its broader advocacy for Risk-Limiting Audits (RLAs) and voter-verifiable paper audit trails. While these practices are presented as bipartisan solutions to election security challenges, they inherently steer policy toward the adoption of proprietary and centralized tools like **ARLO**, which **Verified Voting** endorses despite their opacity and dependency on private vendors.

Verified Voting's collaboration with **DHS** and **CISA** further solidifies its role in directing national election policies. These agencies rely on organizations like **Verified Voting** to lend technical and academic legitimacy to their initiatives, particularly in areas like cybersecurity and post-election audits. **Verified Voting**, in turn, uses this platform to advocate for systems and processes that align with its agenda, even when they fail to address critical vulnerabilities or comply with established federal cybersecurity mandates like **EO 13800**. This dynamic creates a feedback loop where **Verified Voting's** recommendations shape federal guidance, which is then disseminated to state and local election officials, reinforcing the adoption of the same systems and technologies it promotes.

In addition to its federal partnerships, **Verified Voting's** involvement in advocacy coalitions magnifies its impact. Collaborations with groups like **Common Cause**, **the Brennan Center for Justice,** and the **National Election Defense Coalition (NEDC)** allow **Verified Voting** to amplify its messaging and align its efforts with broader networks pushing for similar reforms. These coalitions present a united front in advocating for election security measures like RLAs, effectively sidelining alternative approaches that prioritize decentralized governance and local control. The alignment with these groups raises critical questions about **Verified Voting's** independence and its role in perpetuating a centralized, federally influenced model of election management.

Much like the **Brennan Center, Verified Voting** employs public narratives that appeal to the ideals of fairness, transparency, and civil rights. However, its actions suggest a deeper strategy of weaponizing these narratives to advance systems that erode the very

principles it claims to protect. By presenting itself as an impartial expert, **Verified Voting** lends credibility to policies and technologies that compromise voter anonymity, limit public access to essential election records, and concentrate oversight within federal and private frameworks. This approach not only misleads the public but also mobilizes activists and policymakers to support reforms that ultimately undermine the transparency and accountability necessary for democratic governance.

Verified Voting's ability to influence government agencies stems from its strategic positioning within a network of federal and private entities. It operates as both an advisor and an advocate, blurring the lines between objective expertise and partisan advocacy. This dual role allows it to shape policy in ways that prioritize the adoption of its preferred systems while marginalizing dissenting voices. By embedding itself into the structures of federal oversight and advocacy coalitions, **Verified Voting** has become a key player in the broader effort to centralize election infrastructure under the guise of reform.

The implications of **Verified Voting's** influence are profound. By collaborating with federal agencies and advocacy networks to promote proprietary technologies and centralized oversight, the organization contributes to a systemic erosion of voter privacy, local autonomy, and public trust. Its role in shaping election policy reflects a deliberate strategy to align with federal and private interests at the expense of transparency and accountability, raising serious questions about the integrity of the electoral systems it claims to protect. This betrayal of the public's trust underscores the urgent need for scrutiny of **Verified Voting's** activities and its broader role in reshaping U.S. election infrastructure.

Verified Voting's deep involvement with private sector collaborations underscores its significant, though often understated, influence on the technological and structural evolution of U.S. election systems. While its public image is built on a foundation of impartiality and advocacy for election security, its engagement with private corporations reveals a strategic alignment that fosters dependencies on proprietary systems and cloud infrastructure. These partnerships are not merely incidental but central to **Verified Voting's** operational model, creating a direct link between its advocacy and the entrenchment of private-sector control over public election processes.

A defining aspect of **Verified Voting's** private sector collaborations is its close relationship with election technology vendors, where it effectively serves as a bridge

between these entities and federal and state policymakers. By endorsing tools like **ARLO** for Risk-Limiting Audits (RLAs) and supporting the integration of technologies hosted on platforms like **Amazon Web Services (AWS)**, **Verified Voting** contributes to the normalization of proprietary election solutions. Unlike open-source alternatives that prioritize transparency and public oversight, these tools introduce layers of opacity that favor vendor control and centralization, moving further away from the decentralized election governance traditionally valued in U.S. elections.

Verified Voting's influence extends into policy advocacy, where it plays a dual role: promoting proprietary solutions while advising federal agencies such as the **Election Assistance Commission (EAC)** and the **Cybersecurity and Infrastructure Security Agency (CISA).** Through these relationships, the organization steers election security standards and guidelines in ways that align with its technological endorsements. This dynamic positions **Verified Voting** as a gatekeeper in determining which systems are adopted, yet it blurs the line between objective advocacy and vested interests. While the organization claims to champion transparency and security, its promotion of proprietary technologies inherently benefits private corporations, raising concerns about conflicts of interest.

Beyond the technical endorsements, **Verified Voting's** collaborations with major corporations like **Microsoft** and **Amazon** deepen its entanglement with centralized systems. These companies, often portrayed as neutral providers of infrastructure and technological expertise, wield significant control over the platforms that manage voter data, digital ballot images, and audit trails. **Verified Voting's** endorsements lend these systems a veneer of legitimacy, obscuring the inherent risks of centralizing critical election infrastructure in private hands. This reliance on corporate platforms further entrenches dependencies that limit public access and accountability, effectively ceding control of electoral processes to entities driven by profit rather than democratic principles.

What sets **Verified Voting's** private sector alliances apart is the subtle but pervasive way these relationships shape public perceptions and policy decisions. By presenting proprietary tools and centralized systems as necessary for election modernization, the organization frames its advocacy as aligned with the public good. However, this framing often ignores the vulnerabilities these systems introduce, such as risks of data breaches, reduced transparency, and the exclusion of critical election records from public access laws. This selective narrative perpetuates a model of election security that prioritizes

efficiency and convenience over foundational principles of voter trust and system integrity.

Verified Voting's role in shaping public narratives is amplified through its strategic positioning within federal advisory networks and advocacy coalitions. By aligning itself with influential entities like **the Brennan Center for Justice, Common Cause,** and the **National Election Defense Coalition (NEDC),** the organization ensures that its technological endorsements are woven into broader election reform efforts. This integration into larger networks not only magnifies its reach but also shields its advocacy from critical scrutiny by embedding it within a collective narrative of bipartisan reform and technical necessity.

Ultimately, **Verified Voting's** private sector collaborations highlight a critical tension between its stated mission and its operational realities. While it publicly advocates for secure and transparent elections, its deep ties to proprietary systems and centralized frameworks undermine these very ideals. This contradiction raises fundamental questions about the organization's role in shaping U.S. election infrastructure, as its actions contribute to a systemic shift away from public accountability and decentralized governance. By embedding itself into the core of election reform efforts, **Verified Voting** exemplifies the risks inherent in allowing private interests to dominate public electoral systems, calling for a reevaluation of its influence and the broader trends it represents.

Common Cause

Common Cause has positioned itself as a champion of public trust and electoral integrity, actively advocating for RLAs as a fundamental element of election reform. This advocacy, particularly visible during the period leading up to and following the 2019 convening hosted by **Microsoft**, aligns the organization with a network of technologists, policymakers, and private entities who together crafted the RLA framework. The irony is glaring: while marketed as an effort to enhance transparency and accountability, RLAs operate on assumptions and methodologies that obscure the very transparency they claim to uphold.

From a strategic standpoint, **Common Cause's** lobbying efforts for RLAs represent a calculated attempt to align themselves with the zeitgeist of election security and democratic reform. They have partnered with entities such as **Verified Voting**, the

Brennan Center for Justice, and the **National Election Defense Coalition** to present RLAs as a statistical safeguard against electoral fraud. Yet, this advocacy fails to address the foundational flaw of RLAs: they only test the accuracy of the tabulation system under the assumption that every ballot in the pool is legitimate and free from fraud. This oversight renders RLAs incapable of detecting systemic issues, such as fraudulent ballots being introduced into the chain of custody or discrepancies in voter rolls—issues that are fundamental to genuine electoral transparency.

Common Cause's advocacy is particularly ironic given their self-styled role as defenders of democracy. They have failed to recognize or acknowledge that RLAs, by design, exclude key elements of accountability such as public access to cast vote records (CVRs) and verifiable audit trails. Instead, RLAs rely heavily on proprietary systems like **ARLO**, which centralize data and remove it from meaningful public scrutiny. This system not only perpetuates vulnerabilities but also destroys the premise of voter anonymity, undermining the constitutional and human rights they purport to defend.

The role of academia and social activism within **Common Cause's** platform further highlights the performative nature of their agenda. The organization's reliance on academic endorsements and statistical rhetoric provides a veneer of credibility, but this reliance often ignores practical realities. For example, academics supporting RLAs have frequently focused on the statistical elegance of the model without engaging with its operational flaws or systemic vulnerabilities. This disconnect between theory and practice underscores a troubling trend: the prioritization of ideological validation over empirical scrutiny.

Their timeline of advocacy offers another critical insight. **Common Cause** began ramping up its lobbying for RLAs during a period when election security was gaining national attention, leveraging the fear of foreign interference and systemic vulnerabilities to push their agenda. By aligning with federal agencies and private corporations, they ensured that RLAs would become embedded in election reform initiatives nationwide. However, this timeline also reveals their complicity in bypassing federal cybersecurity mandates such as **EO 13800**, which required compliance with the **NIST Cybersecurity Framework.** Instead of addressing these standards, Common Cause promoted a system that centralizes control within private, proprietary frameworks, often at odds with established national security protocols.

The contradictions in **Common Cause's** platform are not merely ironic—they are emblematic of a deeper problem within election advocacy circles. Their focus on "social justice" reform and performative transparency has blinded them to the real-world consequences of their policies. By advocating for RLAs without addressing their systemic shortcomings, **Common Cause** has contributed to a framework that obscures accountability, destroys voter trust, and facilitates centralized control over elections.

Exposing these contradictions is essential for dismantling their platform. By demonstrating that their advocacy for RLAs does not achieve the transparency or trust they claim, we can undermine their legitimacy and highlight the broader failures of the electoral reform movement. **Common Cause's** alignment with RLAs, far from protecting democracy, has compromised its integrity. Their role in this system is not one of reformers but enablers of a deeply flawed model that undermines the very principles they claim to uphold.

The Brennan Center for Justice

The Brennan Center for Justice has emerged as one of the most vocal proponents of Risk-Limiting Audits (RLAs), actively shaping national and state election policies through advocacy, public messaging, and strategic collaborations. Its role in promoting RLAs reflects a broader strategy to centralize election management while cultivating a public perception of transparency and accountability. However, a closer examination of their actions reveals significant contradictions and a troubling reliance on flawed methodologies that undermine the integrity they claim to uphold.

At the heart of the **Brennan Center's** advocacy is the assertion that RLAs are statistically robust tools for post-election verification. By leveraging the credibility of academic studies and their reputation as a nonpartisan policy institute, the organization has presented RLAs as an indispensable solution to bolster voter confidence and election integrity. Their emphasis on the statistical rigor of RLAs is key to their messaging, but this focus masks the foundational flaw in the process: RLAs assume the legitimacy of all ballots being audited. This critical oversight renders the audits incapable of detecting systemic fraud, such as the introduction of illegitimate ballots or compromised voter rolls, turning them into exercises in validating tabulation rather than ensuring true electoral integrity.

The Brennan Center's collaboration with entities like **Verified Voting** and **Common Cause** has further amplified its influence over RLA adoption. Together, these organizations have championed RLAs through legislative recommendations, policy papers, and public campaigns. While these partnerships are framed as efforts to enhance election security, they often rely on proprietary tools like **ARLO**, which centralize control over audit processes and limit public oversight. **ARLO's** exemption of cast vote records from public access laws exemplifies **the Brennan Center's** complicity in promoting systems that obscure transparency rather than enhancing it.

The Brennan Center's messaging also reflects a deliberate strategy to shape public perception. Their materials consistently present RLAs as cost-effective and scalable, ignoring the operational and logistical challenges they impose on under-resourced election offices. This narrative, reinforced by the organization's status as a thought leader, effectively gaslights the public into viewing RLAs as a comprehensive solution, while significant vulnerabilities remain unaddressed. Concerns about ballot legitimacy, voter roll integrity, and access to meaningful audit data are either dismissed or omitted, fostering a false sense of security in the electoral process.

Their involvement in events like **Microsoft's** January 2019 convening underscores the depth of their integration into the network of stakeholders driving centralized election management. The timing of this advocacy, coinciding with a national push to federalize election systems after the 2016 election, suggests a calculated effort to align RLAs with broader election security initiatives. However, this push has often come at the expense of state and local autonomy, with RLAs embedded into systems that fail to comply with federal mandates like **EO 13800** or the **NIST Cybersecurity Framework.**

The Brennan Center's role in advancing RLAs reflects not just a commitment to election reform but a willingness to overlook the systemic risks associated with their adoption. Their advocacy aligns with the interests of corporate stakeholders and federal agencies, promoting centralized control and proprietary technologies under the guise of transparency. By positioning RLAs as a cure-all for election security, **the Brennan Center** has effectively obscured the inherent vulnerabilities of these systems, contributing to an electoral infrastructure that undermines public trust and accountability.

This duplicity—publicly championing transparency while facilitating centralized control—highlights the systemic contradictions in **the Brennan Center's** platform. Their role

in shaping the narrative around RLAs is not one of a neutral observer or reformer but of an active participant in a broader strategy to reconfigure election systems in ways that prioritize control over genuine accountability. Their actions demand scrutiny, as they exemplify the broader failures and compromises that define modern election reform efforts.

The Brennan Center for Justice leverages its reputation as a premier legal and policy think tank to assert significant influence over the legislative and regulatory frameworks governing election security. Its foundation in legal expertise uniquely positions the organization to shape the trajectory of electoral reform, with Risk-Limiting Audits (RLAs) at the center of its advocacy efforts. This emphasis on RLAs as a policy solution reflects not only the **Center's** technical and strategic priorities but also its ability to frame audits as a legal and constitutional necessity, appealing directly to lawmakers and election officials.

The Brennan Center's legal arguments for RLAs frequently invoke constitutional principles, such as the ***Equal Protection Clause*** and ***the fundamental right to vote***. By positioning RLAs as tools to ensure fairness and accuracy in elections, the organization appeals to the broader legal community's interest in upholding democratic principles. This framing is particularly persuasive for state and federal policymakers, as it ties the adoption of RLAs to compliance with constitutional obligations, making their implementation seem both prudent and legally imperative.

Beyond its appeals to constitutional law, the Brennan Center plays a pivotal role in drafting model legislation to embed RLAs into state election codes. These legislative templates are disseminated through partnerships with state associations and advocacy networks, ensuring widespread adoption of their recommendations. The Center's policy papers often detail the legal frameworks necessary to support RLAs, providing election officials with a roadmap for integrating these audits into their procedures. However, this approach frequently sidelines alternative perspectives, prioritizing RLAs without addressing their foundational flaws or the broader systemic vulnerabilities they fail to mitigate.

The Brennan Center's influence extends into regulatory spheres, where its expertise informs the development of administrative guidelines and standards. For instance, its recommendations to federal bodies like the **Election Assistance Commission (EAC)** and the **Department of Homeland Security (DHS)** often include RLAs as critical

components of election security protocols. This involvement gives **the Brennan Center** an outsized role in shaping how election integrity is defined and enforced at the national level.

Despite its authoritative stance, **the Brennan Center's** legal advocacy for RLAs overlooks critical operational realities. Their policy papers and legislative recommendations often emphasize the statistical rigor and efficiency of RLAs while failing to confront the systems' dependency on proprietary software and centralized data management. By framing RLAs as universally applicable solutions, the **Center** minimizes the risks associated with technological and procedural vulnerabilities that undermine the transparency they claim to promote.

Moreover, **the Brennan Center's** legal framing of RLAs as constitutional safeguards can be seen as a strategic maneuver to preempt and counteract critiques of the system. By anchoring RLAs in the language of rights and protections, the organization deflects attention from legitimate concerns about ballot legitimacy, voter roll accuracy, and the exclusion of cast vote records from public scrutiny. This approach allows them to dominate the policy conversation, sidelining dissenting voices and alternative solutions that might better address the systemic flaws in election infrastructure.

The Brennan Center's legal and policy influence underscores a broader trend of centralizing control over election systems under the guise of reform and modernization. By positioning RLAs as essential tools for legal compliance and public trust, the organization has successfully shaped legislative priorities while reinforcing a framework that prioritizes centralized oversight and proprietary technologies. This duality—advocating for transparency while enabling opacity through centralized systems—reflects a calculated strategy that prioritizes institutional control over genuine electoral accountability. Their role as legal architects of RLA policy makes them a critical player in the broader effort to reshape U.S. election infrastructure, often at the expense of the decentralized principles that underpin democratic governance.

The Brennan Center for Justice has built a reputation as a leading advocate for civil rights and democratic reform, presenting itself as a protector of vulnerable communities and a champion of free and fair elections. However, a closer examination of their narratives and actions reveals a troubling reality: the very systems and policies they advocate for undermine the rights they claim to protect. Through carefully crafted propaganda, legislative drafting, and partnerships with unelected federal bodies, **the**

Brennan Center has weaponized the ideals of civil rights to advance an agenda that, at its core, centralizes control, undermines transparency, and circumvents established national security protocols.

Their advocacy is rooted in narratives that resonate deeply with the public, particularly those who are passionate about justice and equality. **The Brennan Center** frames their efforts as necessary to protect marginalized communities, safeguard against voter suppression, and ensure every vote counts. These themes are emotionally compelling and politically potent, but they obscure the practical consequences of the systems being implemented under their guidance. Systems like the Risk-Limiting Audits (RLAs) they fervently promote introduce centralized, opaque mechanisms that strip away voter anonymity and fail to address foundational security concerns. The irony is striking: in their quest to champion equity, they endorse systems that consolidate power and erode the very civil liberties they claim to defend.

The timing of **the Brennan Center's** push for RLAs and related election reforms is critical to understanding their agenda. Between 2018 and 2019, during President Trump's administration, the organization worked to rapidly institutionalize a framework that bypassed national security directives, such as **EO 13800,** and the mandatory **NIST Cybersecurity Framework (CSF)** requirements for critical infrastructure. This framework was presented as a necessary reform to restore public trust in elections but, in reality, served to create a centralized ***"filing system"*** of voting that sidestepped transparency and accountability. By promoting these systems under the guise of civil rights, **the Brennan Center** effectively gaslit the public, using the language of justice to justify the erosion of democratic safeguards.

The Brennan Center's influence extends far beyond advocacy. They actively draft legislation, advise agencies like the **DHS** and **EAC**, and shape policy decisions at the federal and state levels. These unelected influencers hold immense sway over the direction of U.S. election infrastructure, yet they are accountable to no one. Their actions exemplify the broader issue of private organizations exerting disproportionate control over public systems. While cloaking their influence in the language of equity and progress, **the Brennan Center** has played a pivotal role in enabling a system that aligns more closely with authoritarian centralization than democratic principles.

Their narratives are bolstered by partnerships with federal entities like **DHS** and quasi-public bodies like the **EAC** and **CISA**. These organizations, ostensibly tasked with

safeguarding election integrity, often adopt and amplify **the Brennan Center's** messaging. This alignment has allowed **the Brennan Center** to embed its policies into national frameworks, further insulating their flawed systems from scrutiny. By promoting RLAs and other centralized solutions as tools of fairness, they have managed to obscure the fact that these systems fail to meet the federal law at the time of their creation and implementation.

The Brennan Center's actions and messaging reflect a deliberate strategy to exploit public trust and mobilize activists under false pretenses. Their framing of RLAs as civil rights tools taps into the moral and emotional urgency of justice while sidestepping the operational and legal flaws that undermine these very rights. This weaponization of civil rights advocacy has deceived countless Americans into supporting systems that diminish transparency, fail to meet national security standards, and concentrate power in the hands of a few unelected entities.

At its core, **the Brennan Center's** agenda reveals a chilling truth: the fight for civil rights has been co-opted as a vehicle for implementing centralized control under the guise of equity. By drafting legislation, influencing federal agencies, and gaslighting the public with narratives of progress, **the Brennan Center** has orchestrated a massive realignment of election systems that undermines the sovereignty of states and the will of the people. Their approach is emblematic of a broader Marxist strategy to dismantle the decentralized governance that defines American democracy, replacing it with a system that serves the interests of a select few. Far from defending civil rights, **the Brennan Center's** actions have paved the way for their erosion.

The Brennan Center's role in addressing election misinformation represents another facet of its broader strategy to shape public narratives while embedding its flawed election systems. Framing itself as a counterforce to disinformation, the **Center** has taken an active role in combating what it describes as threats to voter confidence and electoral integrity. This mission, while ostensibly noble, is executed in ways that deflect legitimate criticisms of their endorsed systems and reframe dissent as the product of falsehoods rather than substantive concern. By positioning themselves as arbiters of truth, **the Brennan Center** has effectively weaponized the fight against misinformation to consolidate control over election discourse and suppress challenges to their agenda.

Central to **the Brennan Center's** campaign against misinformation is the claim that RLAs and related election reforms are the gold standard for securing elections. By

promoting these systems as foolproof and impervious to manipulation, they aim to neutralize skepticism and dismiss critiques of centralized election systems as baseless. However, this approach conflates genuine disinformation—such as baseless claims of widespread hacking—with valid, evidence-based concerns about the operational vulnerabilities of RLAs, proprietary technologies like **ARLO**, and centralized data systems. This conflation allows **the Brennan Center** to dismiss critiques of their systems as conspiracy theories, insulating their agenda from meaningful scrutiny.

The timing of their anti-misinformation campaigns is particularly telling. Following the heightened scrutiny of the 2016 presidential election, **the Brennan Center** ramped up efforts to control the narrative around election security. This involved not only public-facing campaigns but also collaboration with federal agencies like **DHS**, **CISA**, and the **EAC**. By aligning with these entities, **the Brennan Center** ensured that their messaging was amplified through official channels, giving it the appearance of impartiality and authority. This alignment, however, also meant that dissenting perspectives were systematically marginalized, as **the Brennan Center's** framing became the dominant narrative in election security discourse.

The organization's focus on misinformation extends to how they engage with the public. Through white papers, public statements, and media campaigns, **the Brennan Center** has positioned RLAs as a necessary countermeasure to false claims of election fraud. While this framing resonates with a public increasingly wary of disinformation, it also obscures the reality that RLAs do not address key vulnerabilities like voter roll accuracy, ballot legitimacy, or the risks posed by centralized systems. By framing RLAs as the solution to mistrust in elections, **the Brennan Center** perpetuates a false sense of security while deflecting attention from the systemic flaws of the systems they promote.

Moreover, **the Brennan Center's** anti-misinformation efforts often extend beyond technical claims to moral and emotional appeals. They frame opposition to their endorsed systems as undermining democracy itself, effectively silencing critical voices by equating dissent with an attack on democratic values. This rhetorical strategy not only stifles debate but also reinforces **the Brennan Center's** control over the election security narrative. By casting themselves as protectors of democracy, they obscure the ways in which their policies centralize control, erode transparency, and fail to meet federal cybersecurity standards like those outlined in **EO 13800.**

The organization's approach to misinformation also intersects with its broader civil rights narrative. By linking RLAs and other reforms to the protection of marginalized communities, **the Brennan Center** positions its agenda as morally unassailable. This framing allows them to dismiss critiques of RLAs as not only factually incorrect but also as antithetical to the fight for justice and equity. This dual-layered narrative—grounded in both technical claims and moral imperatives—creates a powerful, if misleading, justification for their agenda.

Ultimately, **the Brennan Center's** fight against misinformation serves a dual purpose. On the surface, it aims to restore public trust in elections and combat falsehoods that undermine confidence in democratic processes. However, beneath this veneer lies a calculated effort to consolidate control over election discourse, deflect criticism of their flawed systems, and embed a centralized, opaque model of election management. By reframing dissent as misinformation, **the Brennan Center** not only insulates its agenda from scrutiny but also perpetuates a system that erodes the very trust it claims to restore. This manipulation of public discourse is emblematic of a larger strategy to reshape U.S. election systems under the guise of reform, while systematically sidelining transparency, accountability, and decentralized governance.

The Brennan Center's unique integration with academia and research institutions represents one of its most potent strategies for advancing its agenda while shielding it from scrutiny. By aligning with academic voices and sponsoring studies that reinforce its narratives, **the Brennan Center** leverages the perceived neutrality and authority of higher education to legitimize its policies. This partnership with academia allows the organization to create a feedback loop where its advocacy appears grounded in objective research, even when the studies themselves reflect selective framing and omissions.

Through academic partnerships, **the Brennan Center** has cultivated an intellectual veneer for policies like Risk-Limiting Audits (RLAs). The organization sponsors research that emphasizes the statistical validity of RLAs while conveniently avoiding discussions about their operational shortcomings or the risks of centralized, proprietary systems. This selective focus creates the illusion of academic consensus, lending credibility to **the Brennan Center's** claims and influencing public officials, policymakers, and media narratives. By funding and amplifying such research, **the Brennan Center** not only shapes the discourse but also sidelines dissenting perspectives that could challenge its agenda.

The **Center's** academic collaborations extend beyond research papers to include panel discussions, conferences, and training sessions where RLAs and related reforms are presented as essential tools for election security. These events often feature prominent election scientists and statisticians whose expertise lends weight to **the Brennan Center's** positions. However, these forums rarely provide space for critical examination of the broader systemic issues introduced by RLAs, such as their reliance on proprietary software or their incompatibility with decentralized election systems.

One of the most striking aspects of **the Brennan Center's** academic strategy is its ability to obscure the political and ideological motivations behind its advocacy. By presenting its policies through the lens of academic rigor, the **Center** deflects attention from its deeper alignment with federal agencies and private stakeholders who stand to benefit from the centralization of election infrastructure. This alignment raises questions about the integrity of the research being promoted, as well as the independence of the academics involved.

The Brennan Center's academic partnerships also intersect with its broader narrative-building efforts. By tying RLAs and other election reforms to themes of equity, transparency, and accountability, the organization frames its advocacy as inherently virtuous and above reproach. This framing is reinforced by the academic studies it sponsors, which often echo the **Center's** talking points and reinforce its messaging. The result is a closed loop of validation, where **the Brennan Center's** policies are continually reinforced by the research it funds and promotes.

This strategy of leveraging academia highlights a key contradiction in **the Brennan Center's** approach. While presenting itself as a champion of transparency and accountability, the organization relies on selective narratives and controlled research to advance its agenda. This approach undermines the very principles it claims to uphold, creating a system where dissenting voices are marginalized, and critical issues are ignored in favor of advancing centralized control.

Ultimately, **the Brennan Center's** integration with academia serves as both a shield and a weapon. It protects the organization from scrutiny by cloaking its policies in the legitimacy of academic research, while simultaneously using that research to advance an agenda that centralizes power and undermines decentralized election governance. This duality is emblematic of the broader contradictions in **the Brennan Center's** role in election reform—contradictions that demand greater scrutiny and accountability.

The Brennan Center's role in drafting and influencing federal and state election policy highlights its strategic position as a behind-the-scenes architect of systemic changes in election infrastructure. Unlike advocacy organizations that focus solely on public awareness, **the Brennan Center** operates at the intersection of legislative drafting, agency guidance, and public policy. This multifaceted approach allows the organization to embed its priorities into the frameworks governing elections at every level, all while circumventing traditional mechanisms of public accountability.

At the federal level, **the Brennan Center** exerts significant influence over agencies like the **Election Assistance Commission (EAC),** the **Department of Homeland Security (DHS)**, and its subsidiary, the **Cybersecurity and Infrastructure Security Agency (CISA).** Through policy recommendations, advisory reports, and public advocacy campaigns, the **Center** shapes these agencies' priorities, particularly around issues like election security and audit protocols. For instance, the **Center's** emphasis on Risk-Limiting Audits (RLAs) and vendor oversight has directly influenced federal election security guidance. However, these contributions often reflect a selective focus on centralized solutions that align with the interests of proprietary vendors and federal control, sidelining alternative approaches that emphasize decentralization and local governance.

At the state level, **the Brennan Center's** impact is even more pronounced. The organization actively drafts model legislation designed to standardize election practices across jurisdictions. These legislative templates frequently emphasize RLAs, voter-verifiable paper audit trails, and enhanced cybersecurity measures. While these proposals are presented as nonpartisan and pragmatic, their practical implementation often involves adopting proprietary technologies and centralized systems that undermine the transparency and accountability **the Brennan Center** claims to champion.

The Brennan Center's drafting of election policy is not limited to technical recommendations; it also reflects a broader ideological agenda. By embedding civil rights language into their policies, the organization frames its proposals as essential for equity and fairness, making them politically unassailable. This framing has enabled **the Brennan Center** to push through policies that centralize control over election infrastructure under the guise of protecting voter rights. However, the practical effect of these policies often runs counter to their stated goals, creating systems that limit public oversight and concentrate power in the hands of unelected officials and private vendors.

This influence is amplified by t**he Brennan Center's** alignment with federal initiatives like **Executive Order 13800,** which mandates compliance with the **NIST Cybersecurity Framework** for critical infrastructure. While **EO 13800** provides a robust standard for election security, **the Brennan Center** has used its provisions selectively, advocating for policies that appear compliant on the surface but fail to address underlying vulnerabilities. For example, the **Center's** promotion of proprietary tools like **ARLO** and internet-based platforms like **OmniBallot** reflects a prioritization of convenience and scalability over adherence to the decentralized principles that **EO 13800** was designed to protect.

The Brennan Center's involvement in election policy extends beyond drafting and advocacy to include lobbying and direct engagement with policymakers. Through reports, briefings, and private consultations, the organization ensures that its priorities are reflected in legislative and regulatory outcomes. This direct access to decision-makers, combined with its public-facing campaigns, allows **the Brennan Center** to shape the narrative around election security in ways that obscure the systemic risks and contradictions inherent in its approach.

By positioning itself as a trusted advisor on election reform, **the Brennan Center** has embedded itself into the very fabric of election governance. Its policies, while framed as solutions to enhance transparency and security, often serve to entrench centralized control and limit public accountability. This dual role—as both a policy architect and an advocacy organization—exemplifies the systemic contradictions at the heart of modern election reform efforts, where the language of progress is often used to justify practices that undermine democratic principles.

The Brennan Center for Justice stands as a stark example of how a non-governmental organization, cloaked in the guise of civil rights advocacy and academic rigor, has become an influential arm of federal government agencies and private interests. By leveraging its reputation and extensive network, **the Brennan Center** has insinuated itself into the heart of election security and public policy, subverting the will of the people while manipulating its supporters into advancing causes that undermine the very rights they believe they are protecting. This organization has evolved into a de facto policy architect for critical infrastructure governance, using its reach, funding, and intellectual veneer to mask the insidious nature of its influence.

Under the guise of protecting democracy, **the Brennan Center** has championed flawed systems like Risk-Limiting Audits (RLAs) while ignoring the systemic vulnerabilities these systems introduce. They have weaponized the language of civil rights and equity, framing RLAs as tools for justice and transparency while deliberately overlooking their inability to detect fraudulent ballots, address compromised voter rolls, or comply with federal cybersecurity standards such as those mandated by **Executive Order 13800**. By framing dissent as misinformation and opposition as an attack on democracy itself, **the Brennan Center** effectively silences legitimate criticism and gaslights the public into believing in reforms that consolidate centralized control and diminish public oversight.

The Center's role extends far beyond advocacy. It actively drafts legislation, influences federal agencies like **DHS**, **CISA**, and the **EAC**, and advises state governments, shaping the national election framework without any direct accountability to the electorate. Its ability to embed its policies into federal and state systems demonstrates a disturbing level of influence for a non-governmental organization. By doing so, it bypasses the checks and balances designed to protect against precisely this kind of overreach, creating a policy environment where unelected entities dictate the direction of national security and election integrity.

This reach is amplified by **the Brennan Center's** deep integration with academia, where it funds studies and collaborates with researchers to reinforce its narratives. These efforts create a feedback loop of validation, where selectively framed studies lend credibility to its agenda, and the resulting policies further entrench its control. This manipulation of intellectual discourse not only undermines the independence of academic research but also deceives the public into believing that its proposals are grounded in impartial evidence rather than ideological objectives.

The consequences of **the Brennan Center's** actions are profound. By advocating for centralized election systems reliant on proprietary technologies, **the Center** has enabled vulnerabilities that compromise voter anonymity, transparency, and the integrity of the electoral process. Its policies prioritize the interests of private corporations and federal agencies over those of the states and the people, eroding the decentralized governance that is foundational to American democracy. This alignment with federal agencies and private stakeholders places **the Brennan Center** at the center of a broader ***RICO-like conspiracy,*** where entities across public and private sectors collaborate to undermine national security protocols and subvert the Constitution.

The lawful implications of **the Brennan Center's** actions cannot be overstated. Its disregard for federal requirements, such as **EO 13800** and the **NIST Cybersecurity Framework**, exposes it to potential violations of national security laws governing critical infrastructure. By shaping policies that sidestep enforceable protections, **the Brennan Center** and its partners have created systemic vulnerabilities that threaten not only the integrity of elections but also the sovereignty of the nation. This willful negligence—or outright complicity—demands accountability, particularly as it relates to the broader network of actors, **including federal agencies, NGOs, private corporations,** and **international stakeholders**, that benefit from this centralized framework.

At its core, **the Brennan Center** embodies the dangers of unchecked influence and ideological manipulation. Its ability to weaponize civil rights rhetoric and academic institutions to advance centralized control reflects a calculated strategy to reshape American governance under the pretense of reform. In doing so, it betrays the very people it claims to protect, exploiting their trust and activism to dismantle the safeguards of democracy. This betrayal is not merely ideological; it is operational, systemic, and legally actionable, requiring scrutiny and accountability at the highest levels. **The Brennan Center's** role in this conspiracy must be exposed for what it is: a deliberate and strategic effort to erode the principles of decentralized governance and empower a network of unelected entities that prioritize control over democracy.

National Election Defense Coalition (NEDC)

The National Election Defense Coalition (NEDC) occupies a unique and strategic position within the broader ecosystem of organizations influencing election policy in the United States. Framed as a bipartisan initiative dedicated to safeguarding electoral integrity, the **NEDC** has established itself as a major force in the advocacy, design, and implementation of election reforms. While its public messaging emphasizes collaboration, security, and equity, the **coalition's** activities reveal a deliberate alignment with federal agencies, private sector stakeholders, and advocacy networks that prioritize centralized control and proprietary technologies over decentralized, transparent governance.

Central to the **NEDC's** agenda is its promotion of Risk-Limiting Audits (RLAs) and related election security measures. The **coalition** has played a pivotal role in drafting audit principles and best practices, often partnering with influential organizations like

Verified Voting, Common Cause, and **the Brennan Center for Justice**. Together, these entities have worked to establish RLAs as a gold standard for post-election verification. However, the **NEDC's** focus on RLAs highlights a broader strategy to institutionalize systems that rely on proprietary software, centralized oversight, and federal alignment, often at the expense of voter privacy and state sovereignty.

The **NEDC's** collaboration with federal agencies such as **DHS**, **CISA**, and the **EAC** further underscores its influence. By working closely with these agencies, the **coalition** has positioned itself as a critical advisor on election security, shaping federal guidance that is then disseminated to state and local officials. This partnership allows the **NEDC** to embed its priorities into the national framework for election oversight, effectively centralizing control under the guise of bipartisan reform. However, this alignment also raises significant concerns about the **coalition's** role in bypassing federal cybersecurity mandates, such as those outlined in **Executive Order 13800**, and its willingness to endorse systems that compromise transparency and accountability.

A defining feature of the **NEDC's** approach is its ability to unify disparate stakeholders around a shared narrative of election security. The **coalition** presents itself as a bridge between cybersecurity experts, election administrators, civil rights advocates, and technologists, creating a broad base of support for its initiatives. Yet, this narrative often obscures the practical consequences of its policies, which include the normalization of centralized data systems, the exclusion of cast vote records from public access, and the reliance on proprietary audit tools like **ARLO**. By framing these measures as bipartisan solutions, the **NEDC** effectively marginalizes alternative approaches that emphasize local control, public transparency, and decentralized governance.

The **coalition's** role extends beyond advocacy and policy drafting to include public education and narrative control. Through workshops, white papers, and partnerships with academic institutions, the **NEDC** shapes public perception of election security, presenting RLAs and similar reforms as necessary to restore voter trust. However, this messaging often employs selective framing, focusing on the statistical rigor of RLAs while ignoring their dependence on assumptions of ballot legitimacy and their inability to address foundational vulnerabilities in voter rolls and election infrastructure. This approach not only misleads the public but also gaslights critics, framing legitimate concerns as baseless or partisan.

What sets the **NEDC** apart from other advocacy groups is its ability to operate at the intersection of federal oversight, private sector influence, and grassroots activism. By aligning with organizations that share its vision of centralized election systems, the **coalition** amplifies its impact and creates a network of support that spans the public and private sectors. However, this alignment also exposes the **NEDC** to questions about its independence and its complicity in advancing a model of election governance that prioritizes control and efficiency over transparency and accountability.

The timing of the **NEDC's** initiatives further highlights its strategic role in reshaping U.S. election systems. The coalition's push for RLAs and related reforms accelerated in the years leading up to the 2020 election, coinciding with heightened concerns about election security and public trust. By positioning itself as a key player in addressing these challenges, the **NEDC** has been able to institutionalize systems that align with federal priorities while circumventing existing legal and constitutional safeguards.

The **National Election Defense Coalition** represents a powerful and coordinated effort to redefine election security in the United States. Through its collaborations with federal agencies, advocacy networks, and private sector stakeholders, the **coalition** has played a central role in embedding centralized, proprietary systems into the electoral landscape. While its public-facing narrative emphasizes bipartisan reform and voter trust, its actions reveal a deeper agenda to consolidate control and sideline transparency, raising significant concerns about the integrity of the systems it champions. The **NEDC's** influence demands close scrutiny, as it exemplifies the broader systemic contradictions and risks inherent in modern election reform efforts.

The National Election Defense Coalition (NEDC)'s unique role as a unifying bridge between diverse stakeholders is one of its most strategically significant traits, enabling it to exert influence far beyond what a single-focused advocacy group could achieve. Unlike other organizations that may specialize in legal reform, technology, or civic engagement, the **NEDC** actively integrates experts, policymakers, and organizations from all these domains into a cohesive effort to shape election security narratives and policies. This cross-sector collaboration positions the **NEDC** as a central hub in the broader network of election reform advocates, giving it unparalleled reach and credibility.

The coalition's ability to connect election administrators, cybersecurity experts, civil rights organizations, technologists, and federal agencies creates a perception of broad

consensus around its initiatives. By fostering these partnerships, the **NEDC** amplifies its influence and ensures that its agenda is integrated into both policy and operational frameworks at multiple levels of government. This approach not only broadens its impact but also shields its initiatives from criticism by presenting them as the product of collective agreement rather than the agenda of a single organization.

One of the key ways the **NEDC** builds these bridges is by hosting and participating in collaborative convenings, workshops, and panel discussions. These events bring together stakeholders with varied expertise and perspectives, creating a forum for discussing and endorsing shared goals. For example, the **coalition's** involvement in promoting Risk-Limiting Audits (RLAs) has included extensive collaboration with statisticians, election officials, and technology providers to refine and advocate for these systems. By integrating input from these diverse sources, the **NEDC** not only strengthens its recommendations but also ensures buy-in from a broad array of actors, making it more difficult for critics to challenge the legitimacy of its proposals.

The **NEDC** also leverages its partnerships to influence public policy directly. By working with entities like **Verified Voting** and **the Brennan Center for Justice,** the **coalition** extends its reach into state legislatures and federal agencies, advocating for policies that reflect its priorities. These collaborations allow the **NEDC** to present its initiatives as bipartisan and broadly supported, further enhancing their appeal to lawmakers and election officials. However, this perceived bipartisanship often masks the underlying centralization and privatization embedded in the **coalition's** proposals.

Another unique aspect of the **NEDC's** bridging role is its ability to align the interests of civil rights organizations with those of technologists and cybersecurity experts. This alignment is particularly significant because it unites two groups that often operate in separate spheres: those advocating for voter equity and access, and those focused on technical and operational election security. By framing its initiatives as addressing both equity and security, the **NEDC** creates a powerful narrative that resonates with a wide range of stakeholders. However, this framing can also obscure the contradictions between these goals, particularly when centralized systems compromise local control and voter anonymity.

The coalition's partnerships with federal agencies further illustrate its bridging role. By collaborating with **the Department of Homeland Security (DHS)** and its **Cybersecurity and Infrastructure Security Agency (CISA)**, the **NEDC** helps to align

state and local election practices with federal priorities. This alignment often includes the adoption of centralized data systems and proprietary technologies, which, while marketed as secure and efficient, raise significant concerns about transparency and accountability. The **NEDC's** ability to facilitate these partnerships highlights its strategic importance in the federalization of election oversight.

The **NEDC's** role as a unifying bridge allows it to shape election security discourse and policy in ways that few other organizations can match. By integrating diverse stakeholders into a cohesive network, the **coalition** creates the appearance of widespread consensus while advancing an agenda that centralizes control and undermines the principles of decentralized governance. This unique approach makes the **NEDC** a powerful actor in the ongoing transformation of U.S. election systems, with implications that extend far beyond the specific policies it promotes.

The National Election Defense Coalition (NEDC) wields its bipartisan branding as both a shield and a weapon, navigating politically sensitive landscapes while advancing policies that consolidate centralized control over election systems. Unlike overtly partisan organizations, the **NEDC's** emphasis on bipartisan collaboration creates the illusion of neutrality, granting it a privileged position in public and policymaking spheres. This strategic positioning allows the **coalition** to advocate for reforms like Risk-Limiting Audits (RLAs) and other centralized oversight mechanisms without facing the level of scrutiny that might be directed at more transparently ideological entities.

The coalition's bipartisan image is, in practice, a tactical maneuver that masks its alignment with federal priorities and private sector interests. By framing RLAs as purely technical solutions to election security challenges, the **NEDC** sidesteps the deeper implications of their adoption, including their reliance on proprietary technologies, centralized data control, and opaque processes that erode voter trust. This deliberate obfuscation enables the **coalition** to advocate for systems that fundamentally compromise the transparency and accountability they purport to enhance.

One of the **NEDC's** unique strategies lies in its ability to craft narratives that resonate across ideological divides, positioning RLAs and similar reforms as universally beneficial. By appealing to concerns about election integrity and voter confidence, the **coalition** creates a bipartisan consensus around reforms that, in reality, centralize control and limit public oversight. This approach effectively co-opts the language of civil rights

and democracy to advance systems that prioritize efficiency and federal alignment over voter autonomy and decentralized governance.

The **NEDC's** involvement in drafting audit principles and model legislation exemplifies its role in shaping the infrastructure of election reform. While these documents are presented as collaborative efforts to enhance transparency, they often embed systemic vulnerabilities that align with the interests of private vendors and federal agencies. For instance, the **coalition's** endorsement of proprietary RLA tools like **ARLO** introduces centralized oversight mechanisms that restrict public access to election records, undermining the very transparency these audits are supposed to provide.

The **coalition's** bipartisan branding also allows it to obscure the broader implications of its policies. By presenting RLAs as technical solutions rather than political tools, the **NEDC** avoids addressing their foundational flaws, such as their reliance on assumptions of ballot legitimacy and their inability to detect systemic issues like fraudulent ballots or compromised voter rolls. This framing not only deceives the public but also mobilizes activists and policymakers to support reforms that erode constitutional, international, and human rights under the guise of protecting democracy.

Another unique aspect of the **NEDC's** tactical advocacy is its alignment with federal agencies like **DHS** and **CISA**, which benefit from the centralization of election oversight. The coalition's collaboration with these entities reinforces its role as a bridge between federal mandates and state-level implementation, effectively federalizing election systems without direct accountability to voters. This alignment allows the **NEDC** to advance policies that sidestep national security requirements, such as those outlined in **EO 13800**, while framing these reforms as necessary for protecting elections from foreign interference and cyber threats.

The **NEDC's** role in shaping public perception is equally critical. By leveraging its bipartisan branding, the **coalition** builds a broad base of support for its initiatives, often mobilizing grassroots activists to advocate for reforms that ultimately undermine the very principles of voter trust and transparency. This gaslighting of the public perpetuates a false narrative of progress, where systemic vulnerabilities are overlooked, and centralized control is normalized.

In essence, the **NEDC's** bipartisan positioning is not merely a tool for navigating political sensitivities but a calculated strategy for advancing centralized election systems under the guise of nonpartisan reform. By crafting narratives that appeal to both sides of

the political spectrum, the **coalition** obscures the deeper implications of its policies, embedding systemic vulnerabilities into the fabric of U.S. election systems while presenting itself as a champion of democracy. This duality is central to its role in perpetuating the flawed systems it claims to reform, demanding a closer examination of its true objectives and the long-term consequences of its advocacy.

The National Election Defense Coalition (NEDC) stands apart in its ability to craft policy frameworks that subtly embed centralized control mechanisms under the guise of bipartisan election reform. What distinguishes the **NEDC** is not just its technical expertise but its deliberate use of legal and operational templates designed to entrench specific systems and tools across state and local jurisdictions. These frameworks are presented as universal best practices, yet they often prioritize proprietary technologies and federal alignment, steering election oversight away from decentralized governance and public accountability.

Rather than openly advocating for controversial measures, the **NEDC** leverages its collaborative approach to weave centralized oversight into the very fabric of its recommendations. The **coalition** doesn't merely propose principles for election security—it actively constructs legislative templates and procedural guidelines that state and local election officials are encouraged to adopt wholesale. This tactic allows the **NEDC** to bypass rigorous debate and public scrutiny, as these templates often carry the implied endorsement of a bipartisan coalition, lending them unearned legitimacy.

What makes the **NEDC's** frameworks particularly insidious is their focus on embedding centralized tools and processes into ostensibly decentralized systems. These templates often advocate for the adoption of centralized databases, third-party audit tools, and standardized practices that require dependency on private vendors or federal agencies. By doing so, the **coalition** ensures that its frameworks are not only adopted but become the default for election oversight, making alternatives practically infeasible for resource-constrained local governments.

The coalition's drafting process is also marked by its selective use of evidence and expertise. By collaborating with entities like **the Brennan Center for Justice** and **Verified Voting,** the **NEDC** creates the appearance of broad, expert-driven consensus. However, this consensus often excludes dissenting voices that advocate for decentralized, open-source, or voter-driven solutions. Instead, the **coalition** emphasizes

the technical complexity of its proposals to obscure their implications, framing them as non-negotiable steps toward modernizing election infrastructure.

The **NEDC's** frameworks are particularly notable for their emphasis on federal alignment. By aligning state-level practices with federal cybersecurity guidelines, the **coalition** effectively federalizes aspects of election oversight without requiring explicit federal mandates. This alignment is often couched in language about protecting elections from foreign interference or cyber threats, appealing to fears that deflect attention from the centralization and privatization these frameworks facilitate.

Furthermore, the **NEDC's** use of civil rights rhetoric to promote its frameworks adds another layer of complexity to its strategy. By presenting its reforms as essential for equity and inclusion, the coalition mobilizes public and activist support for measures that, in reality, often limit transparency and increase centralized control. This duality—a commitment to civil rights paired with the promotion of systems that erode voter autonomy—exemplifies how the **NEDC** manipulates public perception to advance its agenda.

The **coalition's** influence is not limited to state governments; it extends into federal agencies, where it shapes national standards for election security. Through its partnerships with **CISA**, **DHS**, and the **EAC**, the **NEDC** ensures that its frameworks are integrated into federal guidelines, creating a top-down approach to election oversight that undermines the autonomy of local jurisdictions. This integration makes it increasingly difficult for states or counties to reject the **coalition's** proposals, as federal alignment becomes a prerequisite for funding or technical support.

The **NEDC's** role in drafting policy frameworks is a calculated effort to entrench centralized election systems under the guise of bipartisan reform and technical necessity. By crafting templates that prioritize private sector dependencies and federal alignment, the coalition creates a self-reinforcing system that marginalizes alternative approaches and cements its influence over U.S. election infrastructure. This strategy not only reshapes how elections are conducted but also challenges the fundamental principles of decentralized governance and public accountability, raising profound questions about the long-term implications of its advocacy.

The National Election Defense Coalition (NEDC)'s involvement in funding and resource mobilization for election security reveals a strategic alignment with key donors, private foundations, and federal agencies that influence the distribution of resources

across the electoral landscape. Unlike other organizations that primarily focus on policy or advocacy, the **NEDC** positions itself as a critical intermediary, advocating for increased financial investment while simultaneously steering these funds toward centralized systems and proprietary technologies. This dual role amplifies its influence, allowing it to shape not only the policies but also the operational realities of election security.

At the state and federal levels, the **NEDC** has lobbied aggressively for substantial increases in election security funding. Its messaging often emphasizes the need for modernization, highlighting vulnerabilities in aging voting systems and the purported benefits of adopting new technologies. This advocacy creates a narrative of urgency that aligns with the interests of private vendors and federal agencies, both of which stand to benefit from the influx of resources. By framing its proposals as essential for protecting democracy, the **NEDC** ensures that funding initiatives are viewed as nonpartisan and uncontroversial, further insulating them from scrutiny.

The **coalition's** financial strategy also involves leveraging relationships with major private donors and philanthropic organizations. Among its notable supporters is **the *Democracy Fund***, a nonprofit foundation heavily involved in election-related grantmaking. **The *Democracy Fund's*** emphasis on fostering voter confidence and modernizing election systems dovetails with the **NEDC's** goals, creating a shared agenda that prioritizes centralized solutions. Similarly, the ***Rockefeller Brothers Fund*** and ***the Open Society Foundations*** have contributed to initiatives aligned with the **NEDC's** objectives, providing funding for research, public education campaigns, and technical assistance programs that promote centralized election oversight.

Global partnerships also play a role in the **NEDC's** funding ecosystem. Corporations like **Microsoft**, through its ***Defending Democracy Program,*** have directly supported initiatives that align with the coalition's agenda, including the promotion of Risk-Limiting Audits (RLAs) and other centralized audit mechanisms. These partnerships introduce significant questions about the influence of multinational corporations on U.S. election infrastructure, particularly given the reliance on proprietary systems hosted on platforms like **Microsoft Azure**. The involvement of such corporations creates dependencies that extend beyond financial support, embedding private interests into the core of election security strategies.

In addition to direct funding, the **NEDC** has secured support through federal grant programs aimed at bolstering election infrastructure. These programs, administered by agencies like the **Department of Homeland Security (DHS)** and the **Election Assistance Commission (EAC)**, channel resources into state and local governments for cybersecurity enhancements, audit implementation, and system upgrades. The **coalition's** role as a facilitator in these processes allows it to influence how these funds are allocated, often steering them toward systems and technologies that align with its priorities. This dynamic not only centralizes control but also creates long-term dependencies on federal funding and oversight.

The **coalition's** advocacy for increased funding often includes partnerships with organizations like **Verified Voting, Common Cause**, and **the Brennan Center for Justice,** amplifying its calls for resource mobilization through coordinated campaigns. These collaborations present a unified front that masks the underlying alignment with private sector interests and centralized frameworks. By working in concert with these entities, the **NEDC** ensures that its funding priorities are adopted at multiple levels of government, further entrenching its influence over election security policy and practice.

One of the most troubling aspects of the **NEDC's** funding strategy is its focus on proprietary technologies. By advocating for systems like **ARLO** and platforms hosted on corporate infrastructure, the **coalition** effectively channels public funds into private hands. This redirection of resources not only enriches vendors but also limits the ability of states and localities to pursue independent, open-source, or decentralized solutions. The reliance on proprietary tools creates a feedback loop where the need for ongoing support and updates locks jurisdictions into long-term contracts with private providers, undermining the autonomy of local election officials.

The NEDC's role in funding and resource mobilization for election security is a calculated effort to shape the financial landscape in ways that prioritize centralized control and private sector interests. Through its relationships with philanthropic foundations, global corporations, and federal agencies, the coalition has positioned itself as a gatekeeper for election security funding, directing resources toward systems that align with its agenda. This strategy not only consolidates its influence but also raises critical questions about the transparency and accountability of the funding processes it advocates for. The NEDC's financial entanglements highlight the broader systemic risks of allowing private and global interests to dictate the allocation of resources in U.S. election infrastructure.

The intricate web of relationships among **the National Election Defense Coalition (NEDC), the Democracy Fund, the Rockefeller Brothers Fund, the Open Society Foundations**, and key players like ***Microsoft's Defending Democracy Program*** reveals a coordinated effort to influence election security policy and practice. These entities operate under the guise of bolstering democracy and safeguarding electoral integrity, yet their intertwined roles and actions suggest a deeper alignment with centralized oversight and proprietary control.

The Democracy Fund, established by eBay founder Pierre Omidyar, plays a pivotal role in funding organizations that advocate for election reforms, including those closely tied to Risk-Limiting Audits (RLAs) and centralized systems. The fund's support for entities like **the Brennan Center for Justice** and **Common Cause** enables these groups to promote policy changes and develop resources that align with a nationalized vision of election management. **The Democracy Fund's** influence extends beyond mere financial contributions; its grants amplify the voices of **key stakeholders,** allowing them to shape public discourse and policy frameworks in ways that prioritize modernization over accountability.

Similarly, **the Rockefeller Brothers Fund's** focus on democratic practice positions it as a significant player in supporting organizations advocating for systemic reforms. ***Its funding priorities, exemplified by initiatives like "Our Common Purpose," aim to strengthen democratic institutions but often align with centralized, federally influenced election oversight models. By supporting the Brennan Center for Justice and related initiatives, the Rockefeller Brothers Fund contributes to the institutionalization of practices that undermine local autonomy while presenting them as necessary for democracy's resilience.***

The Open Society Foundations (OSF), founded by George Soros, adds a global dimension to this network. OSF's significant investments in civic engagement and election integrity in the United States align with its broader mission of promoting governance reforms worldwide. Through funding projects like those of the Brennan Center and Verified Voting, OSF reinforces narratives that centralize election oversight under the pretext of combating disinformation and ensuring equity. Its influence on U.S. election infrastructure raises critical questions about the role of global philanthropic entities in shaping domestic democratic processes.

Microsoft's Defending Democracy Program represents the technological linchpin in this network, integrating proprietary systems like ***ElectionGuard*** into election infrastructure. By collaborating with advocacy organizations and election technology vendors, **Microsoft** not only advances its technologies but also positions itself as an indispensable player in modernizing elections. The program's focus on combating cyber threats and disinformation is framed as a public good, yet it simultaneously creates dependencies on private platforms like **Microsoft Azure,** centralizing control over critical election data.

The relationships among these entities are not incidental; they are strategically cultivated to align efforts across funding, advocacy, and implementation. **Common Cause, Verified Voting,** and **the Brennan Center for Justice** serve as the operational and public-facing arms of this network, driving policy recommendations and public education campaigns that normalize centralized and proprietary election systems. The **NEDC's** role as a coordinator and unifier amplifies these efforts, ensuring that their shared agenda is embedded into state and federal election policies.

These organizations leverage their combined resources to craft a narrative that presents RLAs and similar reforms as indispensable for election security. However, this narrative often obscures the foundational flaws of these systems, such as their reliance on proprietary technologies, their exemption of key election records from public access, and their inability to address systemic vulnerabilities like compromised voter rolls or fraudulent ballots. By co-opting the language of equity and civil rights, these entities mobilize public and policymaker support for reforms that ultimately concentrate power in the hands of a few.

The funding mechanisms behind this network reveal a deliberate strategy to centralize control while maintaining the veneer of democratic reform. ***By pooling resources from philanthropic foundations, global corporations, and federal grants, these entities create a feedback loop that reinforces their agenda at every level of government. This system not only sidelines alternative approaches but also institutionalizes dependencies on private vendors and centralized oversight, eroding the principles of local control and public accountability that are foundational to U.S. elections.***

The interconnected efforts of the **NEDC**, **the Democracy Fund, the Rockefeller Brothers Fund, the Open Society Foundations, and** ***Microsoft's Defending Democracy Program*** represent a convergence of advocacy, funding, and technology that

reshapes election security under the guise of reform. While their messaging emphasizes resilience and integrity, their actions consolidate power, limit transparency, and compromise the decentralized governance that is essential to a truly democratic process. This network exemplifies how philanthropic influence, corporate interests, and federal alignment can be weaponized to transform election systems, raising profound questions about the long-term implications for voter trust and electoral sovereignty.

The messaging and strategies employed by **the National Election Defense Coalition (NEDC)** and its network of collaborators starkly contrast with the narrative state officials present when confronted with their failure to comply with federal election security mandates. Public records responses from **Secretaries of State (SOS)** across the nation, denying the applicability of federal laws like **Executive Order 13800** and **the NIST Cybersecurity Framework (CSF)** to state-run elections, reveal a deliberate inconsistency. While states dismiss enforceable federal law as irrelevant, they simultaneously adopt policies and practices dictated by advisory agencies and advocacy groups that claim election security is intrinsically tied to national security.

This contradiction exposes a deeply rooted issue: the weaponization of advisory agencies, advocacy organizations, and philanthropic entities to promote narratives that suit their agenda while bypassing enforceable federal laws. The very architects of the Risk-Limiting Audit (RLA) system—along with its implementation arms like **ARLO** and advocacy groups such as **Verified Voting, Common Cause,** and **the Brennan Center**—have emphasized the necessity of a national security framework to justify their reforms. Yet, when it comes to accountability, state election officials dismiss these arguments and retreat behind the assertion of state sovereignty to sidestep compliance with federally mandated national security protocols.

The claim by state election offices that federal laws governing national security, such as **EO 13800**, do not apply to state-run elections is not only a legal dodge but also a glaring contradiction of their operational reliance on federal guidance. The **NEDC** and its collaborators have meticulously tailored their messaging to frame election security as a national security imperative, successfully persuading states to adopt centralized systems, proprietary technologies, and audit frameworks under the guise of protecting democracy. By positioning RLAs as a critical national security measure, these entities have coerced state officials into implementing systems like **ARLO** while ignoring enforceable standards like the **NIST CSF** that would ensure genuine security and accountability.

This duplicity becomes even more troubling when examining the role of global foundations like **the Democracy Fund, the Rockefeller Brothers Fund, and the Open Society Foundations.** These entities fund election security initiatives that prioritize proprietary systems and centralized oversight, creating vulnerabilities that undermine the very national security they claim to protect. For instance, the **ARLO** auditing system, funded and promoted by these organizations, introduces remote-access capabilities that allow for the selective auditing of ballots. This feature, combined with the RLA's statistical reliance on small sample sizes, enables the manipulation of audit outcomes, concealing fraudulent ballots while presenting a façade of integrity.

The reliance on **ARLO** and similar systems reveals the insidious nature of these reforms. By limiting the scope of audits to predefined percentages and allowing remote access to audit systems, bad actors could ensure that fraudulent ballots are excluded from the auditing process entirely. This capability renders the RLA framework a smokescreen, creating the illusion of rigorous oversight while enabling targeted manipulation. This design, embedded within the centralized systems promoted by the **NEDC** and its allies, represents a direct threat to the integrity of U.S. elections.

The broader implications of these dynamics highlight a coordinated effort to sidestep enforceable national security standards while leveraging the language of national security to justify centralized election reforms. Advisory agencies like **CISA** and the **EAC**, alongside advocacy organizations and global foundations, have constructed a parallel framework that prioritizes centralized control and federal alignment over genuine transparency and accountability. This framework, marketed as essential for election security, effectively bypasses the legal and constitutional safeguards designed to protect state sovereignty and voter autonomy.

The pattern of deflection and denial by state election officials is a symptom of this larger strategy. When questioned about their failure to comply with **EO 13800** and the **NIST CSF,** officials parrot the narrative of state sovereignty to evade responsibility. Yet, their operational reliance on federally aligned advisory agencies and the adoption of proprietary systems like **ARLO** demonstrate a complete subjugation to the centralized framework constructed by the **NEDC** and its network. This contradiction underscores the systemic failures and deliberate obfuscations at the heart of the election security apparatus.

In conclusion, the **NEDC** and its collaborators have orchestrated a comprehensive campaign to align election systems with centralized control under the pretext of national security while evading the enforceable standards designed to ensure genuine security and accountability. ***This strategy, funded by global foundations and implemented through proprietary technologies, represents a clear and present danger to the sovereignty of U.S. elections and the rights of its citizens. The deliberate manipulation of state narratives and the systemic vulnerabilities introduced by these reforms demand urgent scrutiny and accountability at all levels of government. This is not merely an issue of election integrity but a fundamental threat to the democratic principles and national security of the United States.***

Participants at the Microsoft Innovation Lab's "Convening"

The Microsoft Innovation Labs "Convening" brought together a cadre of influential players from across the election security landscape, ostensibly to discuss and implement Risk-Limiting Audits (RLAs) as a cornerstone of election integrity. However, this gathering represents a pivotal moment in the establishment of a system that dismantles voter anonymity and centralizes control over election data, placing it within the reach of federal agencies, intelligence operatives, and private cybersecurity firms.

Participants in this convening were not random selections; they were meticulously chosen figures from academia, advocacy groups, state election offices, and private corporations. Each individual brought their expertise and influence to the table, crafting a narrative of security and transparency while simultaneously laying the groundwork for a system that would compromise the very principles they claimed to protect. The collaboration also included organizations with direct ties to the federal government, such as the **Department of Homeland Security (DHS),** and private entities like **CrowdStrike,** which has a documented history of vulnerabilities in its software solutions. The choice of **Microsoft Azure** as the central storage hub for election data highlights the coordinated effort to leverage corporate infrastructure to advance federal oversight of election systems.

This convening is a prime example of how technocratic expertise, political influence, and corporate power were woven together to promote a vision of election reform that

disguises its true impact: the erosion of voter sovereignty. Each participant, by virtue of their credentials and career history, should have been acutely aware of the implications of implementing a system that centralizes and makes voter data queryable, violating privacy protections enshrined in state constitutions, federal law, and international human rights frameworks. Yet, they moved forward, driven by either ideological alignment, career ambition, or a deliberate intent to reshape the electoral landscape in a way that serves centralized power structures.

The Microsoft Innovation Labs convening was more than a meeting; it was a calculated step in the orchestration of a new electoral regime. The participants, knowingly or unknowingly, contributed to a coordinated strategy to undermine democratic processes, using the veneer of security and innovation to mask the centralization of control and the facilitation of mass surveillance capabilities. Their roles, backgrounds, and connections form the blueprint for understanding how this system came into existence and how it continues to operate as a tool for manipulation and control, rather than the safeguard of democracy it purports to be.



TINA BARTON

City Clerk, City of Rochester Hills, Michigan

Tina Barton serves as the City Clerk of the City of Rochester Hills, MI. She holds a Master of Arts in Management and Leadership, Liberty University. Tina is a Master Municipal Clerk and Certified Michigan Municipal Clerk. She was the 2016 Michigan City Clerk of the Year and the 2017 Leader of Leaders in Public Service – Leadership Oakland.

Tina Barton's involvement in the Risk-Limiting Audit (RLA) system is emblematic of a professional trajectory steeped in election administration expertise, which she leveraged to pioneer systems that fundamentally reshaped the handling of voter data under the guise of improving election security. **Barton's** specific contributions to the implementation of RLAs in **Michigan** and her role as a public advocate for these audits reflect an intimate understanding of the systems she helped institutionalize. What sets **Barton** apart is not just her role in piloting **Michigan's** first RLA but her deliberate positioning as a thought leader in election administration, which allowed her to amplify the adoption of systems that compromise voter anonymity and violate constitutional protections.

Barton's direct role in orchestrating **Michigan's** inaugural RLA pilot in **Rochester Hills** in 2018 was a landmark moment in embedding a centralized, queryable ballot tracking system into the state's election infrastructure. This was not merely a clerical act; it involved active collaboration with state and federal agencies, as well as private entities like **Microsoft**, to implement a system that stored voter and ballot data in ways that made it accessible beyond local jurisdictions. As the **chief election officer** in her city, **Barton** would have overseen every aspect of this pilot, from the data collection and sampling processes to the methods of integrating these results into **Michigan's** broader electoral framework. Her hands-on role in the pilot placed her in a position of direct knowledge regarding how these systems violated voter privacy.

Barton's participation as a panelist at the January 2019 **Microsoft Innovation Lab** convening reveals another layer of culpability. Unlike many other participants who may have been tangentially involved, **Barton** arrived at the event with the experience of having implemented an RLA and was therefore positioned as a subject-matter expert. Her insights at this gathering likely carried significant weight, influencing the recommendations and frameworks discussed. **Barton's** role in this convening went beyond passive attendance; as an experienced election official, she provided practical feedback and strategies for scaling RLAs nationwide. This input was critical in convincing state election offices and advocacy groups to adopt these systems, further embedding centralized data management into the national election infrastructure.

Her career accolades and positions of influence also merit scrutiny. As a recipient of the ***Clearie Award for election innovation***, **Barton** used her elevated profile to advocate for RLAs across other jurisdictions, presenting them as a best practice without addressing the inherent risks they posed. Her advisory roles with the **U.S. Election Assistance Commission (EAC)** and **Michigan's Election Security Advisory Commission** gave her access to policy-making circles where she could shape national narratives around RLAs. **Barton's** personal involvement in these advisory roles, coupled with her knowledge of election laws and security protocols, indicates an active and deliberate effort to normalize practices that dismantle voter anonymity.

Additionally, **Barton's** public defense of RLAs in the face of criticism, particularly after the 2020 election, underscores her commitment to maintaining the system she helped design. Unlike other officials who might deflect responsibility, **Barton** consistently

framed RLAs as essential tools for election integrity, sidestepping concerns about the violations of constitutional protections and international covenants on voter privacy. This public-facing advocacy, coupled with her technical expertise, illustrates a dual role as both architect and apologist for a system that enables **state and federal agencies** and **private corporations** to access sensitive voter data.

Tina Barton's actions are uniquely characterized by her deep involvement at every stage of the RLA's development, implementation, and promotion. Her expertise and career achievements, while presented as assets to election integrity, were instrumental in advancing systems that violate voter sovereignty. **Barton's** specific contributions—her leadership in piloting **Michigan's** RLA, her influential role at the **Microsoft convening,** and her continued advocacy for these audits—reflect a calculated use of her knowledge and authority to further a framework that prioritizes centralized control over constitutional protections. Her culpability is not just in her participation but in her active role in shaping and defending a system that has undermined the foundational principles of democratic elections.



SCOTT BORLING

City Clerk, City of Kalamazoo, Michigan

Scott began his career with the City of Kalamazoo in August of 2000 and has served as the City Clerk since 2005. Scott is a Certified Municipal Clerk and holds a M.A. degree in Medieval Studies from Western Michigan University.

Scott Borling, as the **City Clerk** of **Kalamazoo, Michigan**, occupies a unique position in the orchestration and implementation of Risk-Limiting Audits (RLAs). His role extends beyond that of a local election official; he was directly involved in **Michigan's** inaugural RLA pilot in 2018, one of the earliest and most critical steps in establishing a framework that compromises voter anonymity and centralizes control over electoral data. **Borling's** involvement reflects a combination of technical expertise, administrative authority, and strategic participation in national discussions that shaped the RLA's expansion. This deep engagement, coupled with his apparent understanding of election systems, raises serious questions about his foreknowledge and intent.

Borling's leadership in the **Kalamazoo** RLA pilot was not incidental. **Kalamazoo,** selected alongside **Lansing** and **Rochester Hills**, was one of three jurisdictions chosen to conduct **Michigan's** first RLAs, representing the diverse voting equipment vendors

used across the state. **Borling's** city played a pivotal role in this pilot, showcasing the adaptability of RLAs across different voting systems. This was not merely a procedural experiment but a calculated step to normalize the integration of RLAs statewide. As the **chief election officer** for **Kalamazoo, Borling** would have been deeply involved in every facet of the pilot, from overseeing the tabulation and audit processes to liaising with state officials and external stakeholders. His direct oversight ensured that the systems implemented in **Kalamazoo** aligned with the broader objectives of centralizing election data under the pretext of security.

Borling's participation in the 2019 **Microsoft Innovation Labs convening** further underscores his critical role in advancing RLAs. This event, billed as a collaboration among **election officials, cybersecurity experts,** and **academics**, was instrumental in shaping the national discourse around RLAs. **Borling's** presence as a panelist, armed with the firsthand experience of **Kalamazoo's** pilot, provided a practical endorsement of the system. His contributions likely influenced the framing of RLAs as secure and transparent mechanisms for validating election results. However, this public advocacy masked the inherent risks of the system, including the erosion of voter anonymity and the centralized storage of sensitive electoral data on platforms such as **Microsoft Azure.** As someone deeply familiar with election laws and administrative practices, **Borling** could not have been unaware of these implications.

Borling's actions demonstrate a pattern of engagement with initiatives that prioritize technological centralization over decentralized, voter-protective systems. In 2024, he spearheaded the introduction of a high-speed tabulator in **Kalamazoo** during the August primary election, ostensibly to improve efficiency in ballot counting. While this move was celebrated as a technological advancement, it fits within a broader trend of normalizing data centralization and automation in election systems, further exposing voter data to vulnerabilities and external access. **Borling's** willingness to adopt and promote these technologies without addressing the significant privacy and security concerns speaks to either a gross negligence of his responsibilities or a calculated disregard for the constitutional protections governing voter anonymity.

Borling's career and technical expertise place him in a category of election officials who cannot claim ignorance about the consequences of their actions. His extensive involvement in the design and promotion of RLAs, coupled with his role in advancing centralized election technologies, demonstrates a clear understanding of the systems he was implementing. His active participation in panels, pilots, and state-level innovations

reflects a deliberate effort to embed these systems into the electoral infrastructure, making him a central figure in the erosion of voter privacy under the guise of modernization and security.

The question of culpability looms large over **Borling's** actions. As a trusted **election administrator**, his role was to safeguard the integrity and anonymity of the electoral process, yet his contributions have facilitated the opposite. By championing systems that allow for centralized data storage and querying, **Borling** has aligned himself with a network of actors whose actions directly contravene state and federal protections for voter sovereignty. His role in implementing RLAs and promoting high-speed tabulation technologies ties him to a larger framework that prioritizes control and surveillance over transparency and voter autonomy. **Borling's** deep knowledge of election systems and his active participation in their redesign make his actions not merely administrative but instrumental in the creation and perpetuation of a system that undermines the very democratic principles he was entrusted to protect.



BRENDA CABRERA

Director of Elections, City of Fairfax, Virginia

After 31 years working in both large and small Virginia jurisdictions, Brenda knows that securing elections is vital to voter engagement and confidence. In 2018, the City, conducted a pilot for the first Risk-Limiting Audit in the state of Virginia. Brenda Cabrera is a REO and CERA graduate.

Brenda Cabrera, as the **Director of Elections** and **General Registrar for the City of Fairfax, Virginia,** played a pivotal role in advancing the Risk-Limiting Audit (RLA) framework that has systematically eroded voter anonymity under the guise of election security. **Cabrera's** leadership in conducting **Virginia's** first RLA pilot in 2018 and her participation in national forums positioned her as a key figure in normalizing systems that centralize and expose sensitive voter data to **federal agencies, private corporations,** and **intelligence networks**. Her career-long expertise in **election administration** makes her actions deliberate and deeply consequential.

In June 2018, **Cabrera** oversaw the pilot RLA conducted during the Republican primary for the **U.S. Senate** in **Fairfax**. This audit, executed in collaboration with **Verified Voting**, was publicly marketed as a groundbreaking step in enhancing election transparency and security. However, the system **Cabrera** helped to implement did more

than confirm election outcomes; it centralized data on ballots and voter interactions, rendering them accessible to entities far removed from the local jurisdictions constitutionally entrusted with election oversight. **Cabrera**, with over three decades of experience in **Virginia's** electoral system, was well-versed in the legal protections for voter anonymity enshrined in state constitutions and federal law. Her active role in deploying a system that undermines these safeguards cannot be dismissed as a lack of understanding.

Cabrera's participation in the **Microsoft Innovation Lab** convening in January 2019 further underscores her complicity. As a panelist at this event, she contributed to discussions that promoted RLAs as a scalable, national model. Her insights, drawn from the **Fairfax** pilot, were instrumental in shaping the rhetoric and strategies for broader adoption of these audits. **Microsoft's** involvement, with its centralized **Azure cloud services**, ensured that RLAs would embed centralized data control into election systems under the banner of security and modernization. **Cabrera's** endorsement of these systems reflects either a calculated disregard for their implications or a deeper alignment with the agenda to centralize electoral oversight in ways that violate constitutional protections.

As the **President of the Voter Registrars Association of Virginia (VRAV), Cabrera** wielded significant influence over the professional training and policy perspectives of election officials statewide. Her leadership within this organization allowed her to advocate for RLAs as best practices, embedding them into the educational framework for registrars and directors of elections. This position amplified her ability to normalize these audits, sidestepping critical questions about their impact on voter sovereignty and the risks posed by centralized data access. Her role as **Virginia's** local representative on the **Election Assistance Commission Standards Board** further highlights her involvement in integrating federal election priorities into state systems, aligning local practices with broader national trends toward data centralization.

Cabrera's professional credentials, including her status as a **Certified Elections/Registration Administrator (CERA)** and **Registered Election Official (REO)**, highlight her deep understanding of the technical and legal aspects of **election administration**. This knowledge underscores her awareness of the constitutional and statutory protections for voter anonymity that RLAs jeopardize. **Cabrera's** advocacy for RLAs and her role in their implementation demonstrate a conscious decision to prioritize

centralized control and external oversight over the decentralized protections that have historically defined American elections.

Her continued involvement with **VRAV**, as documented in **IRS filings**, shows a sustained commitment to shaping **election administration** in **Virginia**. Even as a **past president, Cabrera** maintains influence in the organization, which remains focused on registrar education and alignment with state and federal election frameworks. This ongoing role ties her directly to the systemic adoption of policies that compromise voter anonymity and consolidate control over election systems.

Brenda Cabrera's career in **election administration** places her at the intersection of expertise and accountability. Her deliberate participation in RLAs, promotion of their adoption through influential forums, and alignment with organizations advocating for centralized election control implicate her in the broader erosion of voter sovereignty. **Cabrera's** actions reflect a clear understanding of the systems she helped design and an active role in embedding these practices into **Virginia's** electoral framework, raising critical questions about her commitment to upholding constitutional protections for voters. Her involvement exemplifies the calculated strategies of those who have contributed to dismantling the foundational principles of electoral anonymity under the pretext of security and modernization.



DR. JUDD CHOATE

State Election Director, Colorado

Dr. Judd Choate is the state election director for Colorado. Judd has a J.D. from the University of Colorado Law School and a Ph.D. in political science from Purdue University. He was a professor of political science at the University of Nebraska and author of a book on political behavior. In a previous life, Judd was a scout for the Kansas City Royals.

Dr. Judd Choate, as **Colorado's Director of Elections** since 2009, is a central figure in the implementation and national promotion of Risk-Limiting Audits (RLAs), a system that has transformed election oversight under the guise of transparency and security. His leadership in making **Colorado** the first state to mandate RLAs statewide in 2017 marks a significant milestone in the shift toward centralized election control, facilitated by systems that compromise voter anonymity and constitutional protections. **Choate's** deep involvement in the technical, legal, and administrative aspects of elections places him in

a unique position of influence, and his actions demonstrate a profound understanding of the implications of the systems he has helped institutionalize.

Choate's oversight of **Colorado's trusted build procedures for voting systems**, as outlined in official state documentation, demonstrates his technical expertise and pivotal role in ensuring compliance with federal and state standards. The **trusted build process,** which involves the secure compilation of election software to **maintain a chain of evidence,** is critical to the operation of RLAs. **Choate's** leadership ensured that **Colorado's** systems were aligned with these requirements, effectively embedding a framework of centralized oversight and technical control into the state's election infrastructure. His role in this process suggests a deliberate alignment with federal cybersecurity initiatives and the adoption of measures that prioritize systemic control over decentralized, voter-protective systems.

As a founding member of the **Department of Homeland Security's Government Coordinating Council (GCC)** and a **former President of the National Association of State Election Directors (NASED), Choate** has leveraged his state-level expertise to influence national election security policy. His participation in these roles allowed him to shape interagency strategies and coordinate with federal entities, such as the **Cybersecurity and Infrastructure Security Agency (CISA),** to promote RLAs and related systems. His involvement in organizing ***"Tabletop the Vote,"*** a **national cybersecurity exercise simulating election-related cyber incidents,** underscores his active engagement in national preparedness efforts. ***These exercises, while ostensibly designed to enhance security, also facilitated the normalization of centralized data access and federal involvement in state election systems.***

Choate's influence extends into the academic realm, where he serves on the **board of the University of Minnesota's Certificate in Election Administration Program**. His educational efforts focus on **training election officials, reinforcing the narratives and frameworks** that support RLAs and **centralized election oversight**. ***This dual role as a practitioner and educator amplifies his reach, embedding these systems into both operational practices and the professional development of future election administrators.***

Despite the public framing of RLAs as tools for enhancing election accuracy, **Choate's** actions reveal a calculated push toward systems that undermine voter anonymity and decentralization. The implementation of RLAs in **Colorado**, coupled with the use of

trusted builds and interagency coordination, has created an infrastructure where voter data is more accessible to federal agencies, private contractors, and intelligence networks. **Choate's** deep technical knowledge and leadership in these initiatives suggest not only awareness of these risks but also active participation in embedding them into the electoral framework.

Dr. Judd Choate's career reflects a pattern of advancing election systems that prioritize control and oversight by centralized authorities over the constitutional and legal protections historically afforded to voters. His roles in state and national election administration, his advocacy for RLAs, and his influence in academic circles position him as a ***key architect*** of the systems that have redefined election security in the United States. While these efforts have been publicly presented as enhancements to transparency and integrity, their broader implications reveal a systematic erosion of voter sovereignty, facilitated by those entrusted to protect it. **Choate's** actions, informed by his expertise and authority, highlight his critical role in the ongoing transformation of the electoral process into a centralized system vulnerable to surveillance, manipulation, and control.



MONICA CRANE CHILDERS

Vice President of Labs, Democracy Works

Monica is an election technology nerd with a background in digital product design and project management. As Vice President of Democracy Works's Labs program she champions collaborative design, partnering with state and local officials to build low-cost, open source solutions to improve the process and experience of voting. Recent projects include Colorado's Risk-Limiting Audit software, the mail ballot tracking solution Ballot Scout, the reporting website ElectionMail.org, and the Election Technology Collaborative.

Monica Crane Childers stands as a key architect in the technological transformation of election processes, leveraging her expertise to develop systems that ostensibly enhance transparency and efficiency while embedding mechanisms that erode voter anonymity and decentralization. Her tenure at **Democracy Works,** where she served as **Director of Government Services** and later **Vice President of Labs**, positioned her at the forefront of initiatives designed to modernize **election administration.** These efforts, however, reflect a deeper alignment with the infrastructure that centralizes control over voter data,

enabling its accessibility to external entities under the guise of security and modernization.

At **Democracy Works, Childers** championed projects like **Ballot Scout,** a tool that allowed voters to track their absentee or mail-in ballots through the postal system. While this initiative was publicly framed as a service to voters, its integration into broader election infrastructure created pathways for centralized tracking and aggregation of voter data. Similarly, **ElectionMail.org,** another platform spearheaded under her leadership, streamlined election-related communications but also facilitated the collection and management of sensitive information across jurisdictions. These projects illustrate how **Childers**' work consistently blurred the lines between service-oriented innovation and the consolidation of voter data into systems accessible to state and federal actors.

Childers' involvement in developing Risk-Limiting Audit (RLA) software further underscores her central role in advancing technologies that compromise voter sovereignty. Her work on these tools, aimed at ensuring the accuracy of election outcomes, was integral to embedding RLAs into election systems. By facilitating the systematic sampling and analysis of ballots, this software enabled the tracking and storage of voter data in ways that directly contravene constitutional protections for anonymity. **Childers**' position as a designer and promoter of these systems indicates her deep understanding of their implications, making her culpability in their deployment all the more significant.

Her participation in the **Microsoft Innovation Lab** convening on RLAs provided her with a platform to influence national discourse on election security. As an experienced technologist, she was uniquely positioned to advocate for the adoption of these systems, using her expertise to align technology providers, election officials, and government agencies. This role extended beyond technical innovation, placing **Childers** at the intersection of public policy and private sector collaboration—a dynamic that has increasingly enabled the centralization of election oversight.

Beyond **Democracy Works, Childers** has continued to shape the narrative of election administration through her role at the **MIT Election Lab**. As **Manager of Measuring Election Administration** and **Election Science**, she contributes to the application of data-driven approaches to election processes. This ongoing involvement reflects her sustained influence in shaping both the infrastructure and the rhetoric around election modernization. Her advocacy for data visualization and collaborative design underscores

her commitment to embedding technological solutions into every aspect of election administration.

Childers' career demonstrates a calculated focus on developing systems that enhance the visibility and accessibility of election data to external entities, often at the expense of voter privacy and decentralized control. Her deep understanding of election law, administrative processes, and technology highlights her foreknowledge of the implications of the systems she has designed and promoted. By aligning with initiatives that prioritize centralized control and external oversight, **Childers** has played a significant role in dismantling the constitutional safeguards meant to protect voter anonymity and the integrity of decentralized elections.

Monica Crane Childers exemplifies the technocratic ambition driving the transformation of election systems under the pretense of modernization and security. Her projects, while innovative on the surface, serve as tools that have fundamentally reshaped the relationship between voters, administrators, and external entities. Her actions, informed by expertise and authority, implicate her in the broader erosion of voter sovereignty, tying her to a network of actors responsible for advancing a system that prioritizes control over constitutional protections.



KAMMI FOOTE

Inyo County Clerk-Recorder & Registrar of Voters

Kammi Foote is the Clerk/Recorder & Registrar of Voters in Inyo County, California. She serves on the Board of Directors of the California Association of Clerks and Elections Officials and regularly contributes to public policy discussions regarding election integrity. Kammi also serves as a Board member on several non-profits with a focus on civic engagement, civil rights and leadership development.

Kammi Foote, as the **Clerk-Recorder and Registrar of Voters for Inyo County, California**, stands out as a central figure in the advancement of Risk-Limiting Audits (RLAs), a system that has fundamentally reshaped the landscape of election administration. Her leadership in conducting RLAs in **Inyo County** reflects her technical expertise and administrative authority, positioning her as both a pioneer and a promoter of systems that centralize voter data and challenge long-standing principles of election anonymity. With an extensive background in election processes, **Foote's** role

extends beyond local implementation to national advocacy and policy influence, amplifying her impact on election systems across the country.

Inyo County, under **Foote's** direction, was among the first in **California** to adopt RLAs. In November 2020, the county conducted its second RLA, employing hand-marked paper ballots and ballot comparison audits. While these audits were heralded as innovative tools to ensure election accuracy, the reality of their implementation introduced mechanisms that consolidated control over voter data and opened pathways for external oversight. **Foote's** active role in these audits—overseeing their design, implementation, and execution—highlights her deep involvement in embedding these systems into **California's** election framework. Given her expertise, **Foote** was undoubtedly aware of the implications of these audits on voter anonymity, raising questions about her prioritization of technological solutions over constitutional protections.

Foote's influence extends well beyond **Inyo County.** Her participation in the January 2019 **Microsoft Innovation Labs convening** placed her among the nation's most influential voices in election security. This event, titled ***"Making Every Vote Count: A Practical Guide to Risk-Limiting Audits,"*** brought together **academics, election officials**, and **private sector representatives** to discuss the national expansion of RLAs. **Foote's** insights, drawn from her experiences in **California**, were critical in shaping the narratives and frameworks promoted at this **convening**. Her advocacy for RLAs as tools for enhancing transparency and trust often sidestepped the broader implications of these systems, which include the centralization of sensitive voter data and its potential exposure to federal agencies and private contractors.

Her career trajectory underscores her deep involvement in election modernization initiatives. In 2021, **Foote** transitioned from her role in **Inyo County** to join the U.S. **Election Assistance Commission (EAC)** as a **senior subject matter expert.** This move further cemented her influence in national election policy, providing her with a platform to shape federal strategies and promote systems like RLAs on a broader scale. Her work with the **EAC** highlights her alignment with federal election modernization efforts, which often prioritize centralization and technological integration over decentralized, voter-focused protections.

Throughout her career, **Foote** has presented herself as a staunch advocate for transparency and public trust in elections. She emphasized the importance of public

observation in election processes and implemented measures such as **homomorphic encryption for cast vote records** to balance privacy with transparency. However, these measures, while appearing protective, ultimately integrated voter data into centralized systems that could be queried and accessed beyond local jurisdictions. **Foote's** expertise in election law and her active role in designing these systems indicate a clear understanding of their implications, aligning her actions with broader initiatives that prioritize systemic control over voter sovereignty.

Kammi Foote's role in election administration reflects a calculated balance between innovation and oversight. Her leadership in RLAs, her participation in **influential convenings**, and her transition to **federal election policy** illustrate a career deeply intertwined with the systems that have redefined election security and administration. While publicly framed as efforts to enhance integrity and transparency, her actions have contributed to a framework that undermines voter anonymity and decentralization, raising critical questions about the priorities and consequences of her work. **Foote's** career exemplifies the complex interplay between expertise, advocacy, and accountability in the evolving landscape of American elections.



ROBERT GILES

Director, New Jersey Division of Elections

Robert Giles has served as the Director of the New Jersey Division of Elections since 2008. He previously worked at the Ocean County Board of Elections. He serves on the Executive Committee of the Election Infrastructure Government Coordinating Council. Robert is a member of the Standards Board for the U.S. EAC and serves as a representative on the Technical Guidelines Development Committee. He served as a member of the DHS Cyber Unified Coordination Group for the 2016 Presidential Election. He is the President of the NASED and previously served as Vice President of the New Jersey Association of Election Officials.

Robert Giles, as the **Director of the New Jersey Division of Elections** since 2008, has been a central figure in advancing Risk-Limiting Audits (RLAs) and shaping election security measures in **New Jersey** and across the nation. His leadership has positioned him as a prominent voice in the transformation of electoral processes, particularly in embedding systems that centralize voter data and increase external oversight under the guise of transparency and security. **Giles**' extensive involvement in the development and promotion of RLAs reveals a calculated effort to integrate these audits into state and

national election frameworks, raising critical questions about his knowledge of their broader implications.

Under **Giles**' direction, **New Jersey** conducted its first RLA pilot in 2019, a milestone in the state's election security efforts. This pilot involved multiple counties, including **Essex, Gloucester, Mercer, Union**, and **Warren**, and was supported by the **New Jersey Attorney General's Office** and the **Office of the State Comptroller**. **Giles** spearheaded the initiative, which was publicly framed as a tool to enhance the accuracy and integrity of election results. However, the RLA system centralized the handling of ballots and voter data, effectively exposing sensitive election information to external agencies and private contractors. Given his role as the state's top election official, **Giles** would have been intimately familiar with the legal and procedural implications of RLAs, particularly their potential to undermine voter anonymity and constitutional protections.

Giles' influence extends far beyond **New Jersey.** He has participated in national panels and summits, including the **Election Audit Summit** organized by the **MIT Election Lab,** where he shared insights from **New Jersey's** RLA pilot. His involvement in these forums reflects his role as a key advocate for RLAs, promoting their adoption as best practices across the country. These engagements highlight **Giles**' strategic positioning within ***national election security discussions***, where he has contributed to ***shaping the rhetoric and policies surrounding election audits***. His advocacy often emphasized transparency and public trust while downplaying the risks of centralized data control and external accessibility.

Giles' work with the **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)** further underscores his alignment with federal election security initiatives. This collaboration provided state and local election offices with cybersecurity resources, ostensibly to protect election infrastructure from cyber threats. However, the integration of **EI-ISAC** into state systems facilitated the sharing of election data with federal entities, raising concerns about the centralization of control over state-run elections. **Giles**' involvement with **EI-ISAC** exemplifies his role in embedding federal oversight into **New Jersey's** election systems, contributing to the erosion of the decentralized structures that have historically safeguarded voter privacy.

As **Director of Elections, Giles** also oversaw efforts to modernize **New Jersey's** voting systems. These initiatives included implementing voting machines that produce a verifiable paper trail, framed as a measure to ensure election accuracy. While these

systems were presented as a safeguard, they also reinforced the infrastructure necessary for RLAs and the centralized handling of ballots. **Giles**' deep knowledge of election law and administrative processes suggests that he was acutely aware of the implications of these technologies, further implicating him in their broader consequences.

Robert Giles' career reflects a pattern of advancing election systems that prioritize centralized control and external oversight over decentralized, voter-focused protections. His leadership in **New Jersey's** RLA pilot, participation in **national election security forums**, and **collaboration with federal agencies** position him as a critical architect in the transformation of electoral processes. While publicly championing transparency and security, **Giles**' actions have facilitated the creation of systems that compromise voter anonymity and align state election practices with federal priorities. His work exemplifies the complex interplay between innovation, advocacy, and accountability in the evolving landscape of American elections. **Giles**' role in these developments raises serious questions about his commitment to upholding the constitutional protections afforded to voters and the integrity of decentralized election administration.

Robert Giles' involvement in the **DHS Cyber Unified Coordination Group (UCG)** during the 2016 election represents a critical aspect of his contributions to **national election security**. As a member of this **high-level coordination group established under *Presidential Policy Directive-41*, Giles** played a significant role in ***responding to and mitigating cyber threats targeting election infrastructure***. ***The UCG was formed to ensure a unified federal response to major cyber incidents, bringing together entities from across the federal government, including DHS, FBI, and other intelligence agencies, alongside state and private sector partners.***

In this capacity, **Giles** was directly engaged in **managing the cybersecurity posture of election systems** during one of the most contentious and scrutinized election cycles in U.S. history. His role involved the integration of federal resources with state-level election offices, a process that significantly increased the flow of information between these entities. However, this also marked a pivotal moment in centralizing federal oversight of elections, with implications for state sovereignty and the independence of local election administration.

As the **President of the National Association of State Election Directors (NASED)**, **Giles** further cemented his **influence on national election policy**. In this role, he was a ***key conduit*** between **state election directors and federal agencies**, facilitating the

adoption of federally recommended practices, including **cybersecurity protocols and audit processes** like RLAs. While this leadership ostensibly focused on enhancing election security, it also reinforced the integration of state election systems into a broader federal framework, aligning state practices with centralized standards that potentially **exposed sensitive election data to federal and third-party access.**

These roles highlight **Giles**' significant contributions to shaping the evolving relationship between federal oversight and state election administration. His participation in the **UCG** and his **presidency at NASED** placed him at the forefront of efforts to redefine election security, embedding federal priorities into state systems under the guise of responding to cyber threats. These actions, while framed as necessary for safeguarding democracy, facilitated the centralization of election oversight and data control, raising questions about their long-term implications for voter privacy and the independence of state-run elections. **Giles**' direct involvement in these initiatives underscores his awareness of the transformative impact of these measures and positions him as a pivotal figure in the federalization of election security during a critical juncture in U.S. electoral history.



LIZ HOWARD

Counsel, Brennan Center for Justice

Liz Howard serves as Counsel for the Brennan Center's Democracy Program. Her work focuses on cybersecurity and elections. Prior to joining the Brennan Center, Ms. Howard served as Deputy Commissioner for the Virginia Department of Elections. Prior to her appointment, Ms. Howard worked as General Counsel at Rock the Vote, a non-profit organization dedicated to engaging young people in politics. Ms. Howard earned her J.D. from the William & Mary School of Law in 2009.

Liz Howard, a prominent figure in election administration, has cultivated a career deeply entwined with the modernization and federal oversight of election systems in the United States. Her tenure as the **Senior Counsel for the Democracy Program** at the **Brennan Center for Justice** at **NYU School of Law** positioned her as a critical advocate for the adoption of Risk-Limiting Audits (RLAs) and other election security measures. While Howard's work is often framed as a defense of democracy, a closer examination reveals her pivotal role in advancing policies that centralize voter data and increase federal and private sector control over election processes.

Howard's contributions to the **Brennan Center's** reports and public engagements emphasize safeguarding elections through systemic reforms. She has been instrumental in advocating for RLAs, a process that inherently involves the aggregation of detailed election data into centralized systems. Her participation in national forums and collaborative efforts, including her role in drafting ***"How States Can Prevent Election Subversion in 2024 and Beyond,"*** underscores her influence in **shaping the national narrative around election security**. However, the adoption of RLAs, coupled with **Howard's** advocacy for extensive data integration, raises significant concerns about the erosion of voter anonymity—a foundational principle of democratic elections.

Howard's involvement extends beyond academic and policy advocacy. She has worked closely with federal and state agencies, including collaborations with the **Department of Homeland Security (DHS)** and the **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)**. These engagements ***facilitated the sharing of sensitive election data across federal networks under the guise of enhancing security.*** Her role in supporting the integration of election systems with federal cybersecurity frameworks highlights her alignment with broader efforts to centralize control over state-administered elections.

As a former election official in **Virginia**, **Howard's** practical experience lends her a level of authority in these discussions. Yet, her transition from state-level administration to national advocacy suggests a calculated shift towards **influencing federal election policies**. Her work with the **Brennan Center** reflects a consistent emphasis on modernizing election infrastructure, often at the expense of state sovereignty and voter privacy. Her contributions to reports like ***"Defending America's Election Infrastructure"*** and her involvement in efforts to regulate private election vendors reveal a pattern of advancing policies that expand federal and private sector influence over electoral systems.

Howard's expertise and legal acumen make her a formidable advocate for these reforms, but they also position her as a key architect of systems that compromise traditional democratic safeguards. Her promotion of RLAs, support for centralized data sharing, and advocacy for increased federal oversight illustrate her role in a larger effort to reshape the electoral landscape. While framed as measures to enhance security and transparency, these initiatives often undermine the decentralized structure that has historically protected U.S. elections from undue influence.

Liz Howard's career is a testament to the complexities of modern election administration. Her work bridges the divide between policy, practice, and advocacy, making her a central figure in the ongoing transformation of election systems. However, her actions also raise critical questions about the long-term implications of these reforms for voter anonymity, state sovereignty, and the integrity of democratic processes. **Howard's** legacy in election administration will likely be defined by her dual role as a protector of electoral integrity and a catalyst for systemic centralization.



MARK LINDEMAN

Senior Science and Technology and Policy Officer, Verified Voting

Mark Lindeman is Verified Voting's Senior Science and Technology and Policy Officer. He has authored several papers on risk-limiting audit methods including "A Gentle Introduction to Risk-Limiting Audits" and "Risk Limiting Audits: Why and How." An expert in post-election auditing, Mr. Lindeman has advised legislators and election officials in several states about audit methods. He is currently the chair of the Coordinating Committee of the Election Verification Network. Mr. Lindeman earned his Ph.D In Political Science from Columbia University.

Mark Lindeman, a prominent voice in **election security** and the **Policy & Strategy Director at Verified Voting**, has played a decisive role in the advancement and implementation of Risk-Limiting Audits (RLAs) in the United States. Through his **academic contributions, advocacy, and practical application** of RLAs, **Lindeman** has positioned himself as a ***critical architect*** of this audit methodology, which has significant implications for election administration, voter privacy, and state sovereignty over election processes.

As a co-author of ***"A Gentle Introduction to Risk-Limiting Audits,"*** **Lindeman** has provided foundational insights into the statistical underpinnings of RLAs. This work, aimed at demystifying the audit process, has served as a guide for election officials and policymakers navigating the complexities of implementing these systems. The paper highlights the mechanics of RLAs, emphasizing their potential to statistically ensure the accuracy of election outcomes by manually examining a randomized sample of ballots. However, it also acknowledges the necessity of detailed ballot manifests and the precise organization of election materials, which inherently increases the centralization of data

—a move that some argue risks undermining voter anonymity and decentralization in election systems.

Lindeman’s role at **Verified Voting** further solidifies his influence. He has actively participated in shaping state and national policy discussions, often advocating for the adoption of RLAs as a gold standard for post-election audits. In his capacity at **Verified Voting, Lindeman** has advised on best practices for integrating RLAs into existing electoral frameworks, ensuring compliance with statistical rigor while addressing logistical challenges. His involvement in state RLA pilot programs underscores his commitment to embedding these processes into the fabric of American election administration.

The files and reports reveal **Lindeman's** extensive collaboration with election officials, academics, and policymakers. In his co-authorship of key documents like ***"Knowing It's Right: A Practical Guide to Risk-Limiting Audits,"*** **Lindeman** lays out actionable steps for the successful implementation of RLAs, from training election officials to deploying appropriate technology. His emphasis on practical application has been instrumental in guiding jurisdictions through pilot programs, where challenges such as ballot retrieval, chain of custody, and voter intent interpretation are tested and refined.

Lindeman’s association with organizations like **Verified Voting** and his participation in **influential convenings**, such as the **Microsoft Innovation Labs** gathering, place him at the nexus of election security advocacy. While his work is framed as enhancing public trust in electoral systems, his advocacy for RLAs aligns with broader efforts to standardize and centralize election processes under federal and private oversight. This standardization facilitates information sharing with entities like the **DHS**, the **EI-ISAC**, and **private contractors**, raising concerns about the erosion of local control and the potential for misuse of voter data.

His career trajectory and extensive contributions to RLAs also point to his deep awareness of their implications. **Lindeman’s** academic and professional credentials suggest a thorough understanding of the balance between transparency and privacy in election systems. Despite this, the widespread adoption of RLAs under his guidance has introduced vulnerabilities, such as the potential linkage of ballots to voters through detailed audit trails and centralized databases. These risks, while often downplayed in public discussions, highlight the trade-offs inherent in the systems **Lindeman** champions.

Mark Lindeman's legacy in election administration is complex. He is both a thought leader in post-election audit methodology and a key figure in the centralization of election systems. His work underscores the tension between improving election transparency and preserving the foundational principles of voter privacy and local control. **Lindeman's** role in the implementation of RLAs exemplifies the dual-edged nature of technological advancements in election security, where gains in statistical assurance can come at the cost of decentralization and anonymity.

Mark Lindeman's *"A Gentle Introduction to Risk-Limiting Audits"* serves as a foundational document for understanding the statistical and procedural mechanics of RLAs. This file delves deeply into the methodology required for RLAs to function effectively, emphasizing the centrality of ballot manifests and the meticulous organization of election materials, including ballots and envelopes. These elements are not auxiliary to the audit process but are its very core, as RLAs rely on precise, granular data management to validate election outcomes with statistical certainty.

At its essence, an RLA seeks to verify election results by comparing a randomized sample of ballots to the reported outcomes. The integrity and reliability of this process hinge on the ballot manifest—a comprehensive record that details the organization, storage, and distribution of ballots within an election jurisdiction. The manifest must include critical information, such as the total number of ballots cast, the locations where they are stored, and their corresponding batches or containers. Without this meticulously prepared document, the random sampling required for an RLA becomes impossible, as auditors cannot identify which ballots to retrieve or how to verify that the sample is representative of the whole.

The document underscores that the success of an RLA depends not only on the statistical sampling process but also on the physical and procedural organization of election materials. Ballots must be stored in a manner that ensures traceability and accessibility. Envelopes, too, play a crucial role, particularly in vote-by-mail systems, where they may contain voter-identifiable information, timestamps, and signatures. The organization of these materials must balance transparency for audit purposes with stringent measures to protect voter anonymity—a challenge that is often understated in public discussions about RLAs.

Lindeman's writing explicitly details how the RLA process integrates these materials into its mechanics. First, the ballot manifest acts as the blueprint for auditors, guiding

them to specific ballots within a batch or container for examination. Election officials must ensure that the manifest is accurate and up-to-date, reflecting the true state of ballots as they were cast and stored. Any discrepancies or gaps in this documentation undermine the audit's credibility and, by extension, public confidence in the election's integrity.

Second, the envelopes and ballots must be handled in a manner that preserves their chain of custody and ensures they are not tampered with during the audit process. **Lindeman** highlights that every step of the RLA process, from the generation of the ballot manifest to the manual examination of individual ballots, depends on a seamless interplay between statistical rigor and physical organization. If ballots or envelopes are misplaced, damaged, or incorrectly logged, the entire audit can be compromised, rendering its results inconclusive or invalid.

The document also discusses the procedural safeguards required to protect voter privacy during RLAs. Because envelopes and ballots often contain sensitive information, their organization must ensure that voter identities cannot be linked to their choices. This requires a careful separation of identifying details during the initial tabulation process and a commitment to maintaining this separation throughout the audit.

Lindeman's work illustrates that RLAs are not merely statistical exercises but are deeply rooted in the physical and procedural realities of election administration. The meticulous organization of ballots, envelopes, and accompanying documentation is not optional—it is a prerequisite for the audit's success. This requirement ties RLAs to a broader system of data management and record-keeping that centralizes control over election materials, raising critical questions about voter anonymity, local oversight, and the implications of such detailed ballot tracking for election integrity.

Lindeman's *"A Gentle Introduction to Risk-Limiting Audits"* reveals that the RLA process is intrinsically dependent on a system that mandates the precise documentation and organization of ballots and envelopes. This interdependence ensures the audit's functionality but also creates a framework that, if misused, could compromise voter privacy and decentralization. The file provides a clear roadmap for implementing RLAs while highlighting the organizational and ethical complexities that underpin their operation.

Mark Lindeman's assertion in ***"A Gentle Introduction to Risk-Limiting Audits"*** that voter identities cannot be linked to their choices once envelopes and ballots are

separated is emblematic of a broader effort to obscure the realities of the RLA process. While the document emphasizes the careful separation of identifying details during tabulation and the maintenance of this separation throughout the audit, the actual mechanisms of ballot and envelope organization tell a different story—one that reveals the potential for digital linkage even after physical separation.

The claim hinges on the idea that once envelopes and ballots are separated, the connection between voter identity and their ballot is permanently severed. However, this argument conveniently ignores the role of digital tracking systems employed throughout the election process. Machines like **Runbeck** or **BlueCrest** envelope sorters play a crucial role in the early stages of processing, imprinting digital identifiers onto envelopes while sorting them into specific batches. These identifiers are not random; they reflect the precise order of the envelopes as they pass through the sorter—batch, box, and position.

When ballots are extracted from these envelopes, election officials maintain the exact sequence established by the sorting machines. This sequential integrity is carried through to the tabulator, where ballots are digitally imprinted again with metadata indicating their batch, box, and position. Despite the physical separation of envelopes and ballots, this meticulous order ensures that the digital imprinting on the cast vote records effectively links ballots back to their corresponding envelopes. The system relies on maintaining the illusion of separation while preserving a digital breadcrumb trail that allows the connection to be reestablished if necessary.

Lindeman's framing of this process omits these critical details, perpetuating the belief that RLAs inherently protect voter anonymity. This misrepresentation serves as a form of gaslighting, designed to reassure the public and policymakers that their votes are secure and private when, in reality, the architecture of RLAs allows for the precise re-linking of voter identities to their ballots. The digital imprints on ballots and envelopes, combined with the centralized storage of voter data in systems like **Microsoft Azure,** provide a framework for querying and correlating this information.

This issue is compounded by the fact that both ballot images and envelope data are often uploaded to the **Secretary of State's office** or directly into **cloud storage systems.** ***These systems, operated by vendors like Microsoft Azure, store voter profiles and election data together, creating a single repository that can be accessed through data-sharing agreements with federal agencies, including DHS, EI-ISAC, MS-ISAC, and***

others. These agreements mandate the sharing of voter data under the guise of election security, effectively granting federal entities and their contractors access to detailed voter profiles and election results.

The implications of this centralized data architecture are profound. By maintaining a digital link between ballots and voter profiles, these systems enable the federal government or other entities to query voting patterns, predict electoral outcomes, and potentially manipulate elections through targeted interventions such as gerrymandering or ballot injection. The very mechanisms that Lindeman portrays as safeguards for transparency and security become tools for surveillance and control, undermining the fundamental principle of voter anonymity.

Mark Lindeman's explanation in the document represents a deliberate sleight of hand, redirecting attention away from the systemic vulnerabilities embedded in the RLA process. By focusing on the physical separation of ballots and envelopes, he obscures the digital realities that allow for re-linking and centralized querying of voter data. This misdirection not only misleads the public but also facilitates the expansion of election systems that prioritize federal oversight and data accessibility over the constitutional protections of voter privacy and election sovereignty.

Mark Lindeman, alongside contributors such as Pamela Smith of Verified Voting, Mark Halvorson of Citizens for Election Integrity Minnesota, Dan McCrea of the Florida Voters Foundation, Lynn Garland, and Vittorio Addona of Macalester College, co-authored "Principles and Best Practices for Post-Election Audits" to establish a standardized framework for conducting post-election audits. This work, endorsed by organizations like the Brennan Center for Justice, Verified Voting, and others, is a cornerstone in the implementation of RLAs across the United States. The document serves not only as a technical guide but also as a policy manifesto, advocating for transparency, accountability, and perceived voter confidence through systematic auditing.

At the heart of the proposed audit framework is the reliance on meticulously documented ballot manifests and robust chain-of-custody protocols. The authors explicitly detail that for RLAs to function, every ballot must be accounted for, tracked, and sorted into specific audit units—batches defined by precincts, machines, or other logical divisions. These manifests act as the foundational map for audits, directing officials to retrieve and inspect a randomized subset of ballots to verify election

outcomes. While framed as a method to ensure accuracy, this structure necessitates a level of centralized organization and digital tracking that inherently compromises voter anonymity. **Lindeman** and his colleagues present this organization as a necessary trade-off for statistical assurance.

The document further underscores the importance of rigorous chain-of-custody procedures. Paper records, from ballots to voter-verified receipts, must be meticulously maintained to prevent tampering, loss, or mismanagement. This extends to the physical storage and transportation of ballots and the digital imprinting of cast vote records, which inherently ties voter data to specific audit batches. Although the authors claim these safeguards preserve voter anonymity, the technical architecture they promote—where ballots are handled and tracked in precise order—creates a pathway for re-linking ballots to individual voters through digital markers.

Pamela Smith and **Mark Halvorson** contribute heavily to the transparency narrative, emphasizing public observation and accessibility throughout the audit process. They advocate for allowing stakeholders to verify procedures, a seemingly democratic approach that paradoxically adds layers of vulnerability by centralizing sensitive data. **Vittorio Addona's** expertise in statistical methodology informs the risk-limiting components, presenting RLAs as mathematically superior to traditional fixed-percentage audits. Yet this statistical rigor depends on the comprehensive tracking and digitization of ballots, elements that expand centralized oversight.

Mark Lindeman's role in this collaboration is particularly significant. His influence is seen in the emphasis on risk-limiting protocols, which align closely with his other writings and advocacy efforts. By promoting RLAs as the gold standard for post-election audits, **Lindeman** ties his academic and policy expertise to the larger agenda of embedding centralized systems into state-level election processes. This approach integrates federal oversight mechanisms through partnerships with entities like **Verified Voting** and endorsements from statistical associations, giving the framework both intellectual credibility and policy traction.

The other co-authors, such as **Dan McCrea** and **Lynn Garland,** contribute perspectives from grassroots advocacy and electoral reform, adding legitimacy to the broader public-facing narrative of the document. However, their collective emphasis on transparency and accuracy often masks the underlying vulnerabilities of the system they propose. By ensuring ballots and their corresponding data are meticulously tracked and digitally

archived, the framework opens doors to potential misuse by federal entities, private contractors, and other actors with access to centralized election databases.

"Principles and Best Practices for Post-Election Audits" reflects a coordinated effort by **Lindeman**, **Smith**, **Halvorson**, and others to reshape election oversight under the pretense of security and transparency. While the document is presented as a technical guide, its deeper implications reveal a push toward systems that consolidate control over voter data and undermine the decentralized safeguards traditionally protecting election integrity. This collaboration exemplifies how intellectual and advocacy efforts converge to normalize systems that centralize power while promoting an image of democratic accountability.

The document ***"BRAVO: Ballot-polling Risk-limiting Audits to Verify Outcomes"***, co-authored by **Mark Lindeman, Philip B. Stark,** and **Vincent S. Yates**, is a cornerstone in the development of risk-limiting audit methodologies, focusing on ballot-polling as an audit mechanism. This approach outlines a method to statistically verify election outcomes while ostensibly avoiding full hand recounts unless absolutely necessary. The process hinges on several key components that expose the tension between transparency, centralization, and voter anonymity, particularly when examined through the lens of its implications on electoral integrity.

BRAVO introduces a sequential approach to ballot-polling, where ballots are randomly selected and manually inspected until there is either sufficient evidence to confirm the reported outcome or a discrepancy significant enough to warrant a full recount. Central to this methodology is the ballot manifest—a detailed inventory that maps every ballot to its storage location. This document highlights the necessity of precise record-keeping, as auditors must rely on the manifest to locate specific ballots. While presented as a logistical requirement, this meticulous organization also enables the possibility of linking ballots back to their original contexts, undermining claims of voter anonymity.

The authors assert that ballot-polling audits require minimal demands on voting systems compared to comparison audits, which necessitate access to detailed cast vote records (CVRs). However, **BRAVO's** efficiency relies on the exact same careful organization of ballots as comparison audits. It requires not only physical order but also robust chain-of-custody protocols to maintain the integrity of the audit process. This dependency on centralized and precise tracking systems mirrors the structure criticized for its potential misuse in broader RLA frameworks.

Stark and Lindeman's approach also emphasizes multi-jurisdictional coordination, with central authorities overseeing audit operations across states or regions. This centralization facilitates the consolidation of ballot data, ostensibly to streamline audit procedures. However, this framework introduces risks associated with data sharing agreements and federal oversight, particularly given the involvement of agencies like **DHS** and contractors like **Microsoft Azure,** where election data is frequently stored. The central authority's role in aggregating ballot manifests and coordinating sampling further entrenches a system where voter privacy could be compromised by centralized data storage and digital tracking.

BRAVO's authors highlight the logistical flexibility of ballot-polling audits, allowing jurisdictions to adjust sample sizes dynamically based on initial results. Yet, this flexibility also demonstrates how deeply interconnected the process is with digital infrastructure. Random sampling relies on algorithms and systems that, if compromised, could skew results. Furthermore, the integration of ballot manifests into centralized digital systems underpins the entire methodology, creating vulnerabilities that could be exploited to trace individual votes.

The discussion on **BRAVO's** historical application further contextualizes its broader goals. By analyzing state-level presidential contests from 1992 to 2008, the authors demonstrate the scalability of their method for large elections. However, the scalability is contingent on precise, centralized coordination and uniform compliance across jurisdictions, which inherently conflicts with the decentralized nature of U.S. elections. The claimed efficiency of **BRAVO** in verifying outcomes often obscures its dependence on centralized oversight and digital infrastructure, raising concerns about its potential for misuse.

Mark Lindeman's role in co-authoring **BRAVO** underscores his long-standing advocacy for RLAs and his intellectual contributions to their statistical underpinnings. His collaboration with **Philip Stark** and others reflects a shared commitment to advancing audit methodologies while simultaneously embedding systems that centralize control over election materials. The dual focus on statistical rigor and logistical practicality often overshadows the broader implications of the **BRAVO** framework, particularly regarding voter privacy and the potential for federal encroachment on state-administered elections.

In summary, **BRAVO** exemplifies the intricate balance between ensuring election accuracy and preserving voter anonymity. While framed as a transparent and efficient audit mechanism, its reliance on centralized tracking systems, digital infrastructures, and federal coordination introduces vulnerabilities that challenge its claims of safeguarding electoral integrity. **Lindeman's** work, as part of this collaboration, reflects both the strengths and inherent risks of embedding such methodologies into the fabric of modern election systems.

A Gentle Introduction to Risk-Limiting Audits- https://docdro.id/AfP18z5

Knowing It's Right: A Practical Guide to Risk-Limiting Audits - Part one - https://docdro.id/9gan6Hr

Knowing It's Right: A Practical Guide to Risk-Limiting Audits - Part Two and Three - https://docdro.id/5n6LNmH

Principles and Best Practices for Post-Election Audits - https://docdro.id/7mT43JT

BRAVO: Ballot-polling Risk-limiting Audits to Verify Outcomes - https://docdro.id/cCkBnpI



JEROME LOVATO

Election Technology Specialist,
U.S. Election Assistance Commission

Jerome Lovato is an Election Technology Specialist at the U.S. Election Assistance Commission (EAC). At the EAC, Mr. Lovato assists jurisdictions with developing processes and procedures for conducting risk-limiting audits. An expert in voting systems, he is a former certified Colorado Election Official and City of Centennial Election Commissioner. Prior to joining the EAC, he served as a Voting Systems Specialist at the Colorado Secretary of State's office for 10 years. Lovato received his Bachelor of Science in Electrical Engineering from the University of Colorado at Denver.

Jerome Lovato's career and actions reveal a deeply entrenched role in the evolving landscape of election systems, particularly as it relates to certification, testing protocols, and the integration of technology within election infrastructure. His trajectory from the **Election Assistance Commission (EAC)**, where he managed the testing and certification program, to his position at **Clear Ballot,** highlights a consistent involvement in critical nodes of the election system pipeline.

Lovato's tenure at the **EAC** was marked by his emphasis on the importance of federal and state certification processes for voting systems. He regularly worked to bridge the gap between state and federal testing standards, ensuring that states adhered to the voluntary guidelines established by the **EAC** while navigating unique state-specific requirements. His influence extended to oversight mechanisms, such as developing protocols for ensuring that wireless capabilities on election tabulators were disabled, a recurring concern addressed in correspondence with state election officials. While this work ostensibly aimed to bolster election security, it also demonstrates how tightly intertwined the **EAC's** guidance is with the vendors responsible for implementing these systems.

As **Director of Certification at Clear Ballot, Lovato's** influence deepened. In this role, he was directly responsible for overseeing compliance with both federal and state certification requirements for election technologies. His work here involved managing the certification lifecycle, which includes the testing of election systems for accuracy, security, and compliance with established guidelines. However, this position also placed him in close proximity to the companies and organizations shaping election technology, blurring the lines between regulatory oversight and industry promotion.

Notably, the correspondence between **Lovato** and officials such as **Stuart Holmes** underscores the ongoing challenges and vulnerabilities in the system. For example, **Lovato's** engagement on issues such as wireless sniffers for penetration testing illustrates a reactive, rather than proactive, approach to election security. While he provided technical insights and industry best practices, these efforts often addressed symptoms rather than root causes of system vulnerabilities.

Lovato’s connections to **Clear Ballot** also introduce questions of conflict of interest. By transitioning from a federal oversight role at the **EAC** to a leadership position within an election technology vendor, **Lovato** exemplifies the revolving door phenomenon that often complicates impartiality in regulatory frameworks. **Clear Ballot’s** products, which include tabulation systems and audit tools, rely heavily on the protocols and certifications he helped establish, creating a potential feedback loop of influence.

In broader terms, **Lovato’s** work is emblematic of the systemic challenges facing election systems. The centralization of certification processes, the reliance on voluntary guidelines, and the tight coupling of public and private sectors have collectively created an environment where transparency and accountability are difficult to achieve. **Lovato's**

career trajectory, while ostensibly dedicated to improving election security, reflects these tensions. His expertise and actions, particularly in the realms of testing and certification, have undoubtedly shaped the current election system landscape, but they also underscore the inherent vulnerabilities introduced by a system that depends on centralized oversight and vendor collaboration.

Jerome Lovato's role within the election system ecosystem is both influential and complex. His contributions to certification protocols and security practices have had a lasting impact, but his career also highlights the systemic vulnerabilities and potential conflicts of interest that continue to challenge the integrity and independence of election systems.

Jerome Lovato's connection to **Stuart Holmes** and his involvement with **Washington's** election systems reveal a deeply strategic alignment that ties federal oversight to state-level election administration through private sector tools. At the **EAC**, **Lovato** worked closely with officials like **Holmes**, providing federal guidance on election security, certification, and the implementation of critical technologies, including risk-limiting audits (RLAs). ***Holmes, a key figure in Washington's OSOS, relied on this guidance to align the state's election systems with federally recommended practices, creating a seamless yet centralized framework for managing elections.***

The relationship between Lovato and Holmes is most evident in the implementation of RLAs, which demanded detailed ballot manifests and precise chain-of-custody protocols. Lovato's federal expertise directly influenced how Washington structured these audits, ensuring that systems met compliance standards but also embedding a level of centralized control that conflicted with the state's historically decentralized electoral processes. Holmes, under Lovato's guidance, adopted RLA tools and methodologies that integrated closely with Washington's centralized VoteWA system, raising concerns about the potential for data accessibility by external entities, including federal agencies and private contractors.

Lovato's transition to Clear Ballot amplified these concerns. At Clear Ballot, Lovato oversaw the certification and deployment of technologies that directly interacted with Washington's election systems. Clear Ballot's tools, including their audit and tabulation systems, depend on granular data tracking and the storage of voter data in structured formats. Holmes' efforts to modernize Washington's election infrastructure through centralized systems like VoteWA created a natural intersection with Lovato's

work at Clear Ballot. This overlap highlights a broader issue of influence, where private vendors and public officials collaborate in ways that prioritize technological integration over voter privacy and system transparency.

The dynamic between Lovato and Holmes also underscores a recurring issue in modern election systems: the blurred lines between oversight and vendor promotion. Lovato's involvement in Washington elections illustrates how federal and state systems increasingly depend on private sector technologies, creating potential conflicts of interest. This reliance on vendors like Clear Ballot to provide compliance-driven solutions aligns with federal mandates but undermines the autonomy of state-level election management.

Jerome Lovato's role in shaping Washington's election systems, particularly in his interactions with Stuart Holmes and his influence at Clear Ballot, demonstrates the systemic entanglement of federal guidance, state implementation, and private sector dependency. While Lovato's contributions ostensibly aim to enhance security and accuracy, they also reveal the vulnerabilities inherent in a system where centralized oversight and vendor reliance supersede the principles of transparency and decentralized electoral integrity.



JOHN MARION

Executive Director, Common Cause Rhode Island

John Marion is the Executive Director of Common Cause Rhode Island, where he serves as the organization's chief legislative advocate and is spearheading efforts to adopt and implement risk-limiting audits in the State of Rhode Island. Mr. Marion has led successful campaigns to reform Rhode Island's campaign finance disclosure laws, amend the Rhode Island Constitution to restore the Ethics Commission's jurisdiction over the General Assembly, and require risk-limiting post-election audits, among others. He received a B.A. from Binghamton University and attended Indiana University for graduate school.

John Marion, as **Executive Director of Common Cause Rhode Island**, represents a key figure in the advocacy for policies that purport to enhance election security and transparency but often result in centralized control over election systems and diminished voter privacy. Under **Marion's** leadership, **Common Cause** has been instrumental in influencing state-level reforms that align with the broader national agenda of organizations such as the **Brennan Center, Democracy Fund,** and **Microsoft's**

election-related initiatives. While **Marion's** work ostensibly focuses on improving voter access and ethical governance, his actions must be critically examined for their role in enabling systemic vulnerabilities and consolidating control over electoral processes.

Marion's tenure at **Common Cause Rhode Island** aligns with significant shifts in the state's election administration, including the implementation of policies that intertwine voter registration databases, ballot tabulation, and audit processes under centralized frameworks. These frameworks, often justified under the guise of "efficiency" and "security," directly mirror the principles promoted by national organizations advocating for Risk-Limiting Audits (RLAs) and digital ballot tracking systems. **Marion's** advocacy for these measures demonstrates either a lack of understanding of their long-term implications or a willful alignment with efforts to institutionalize surveillance-like mechanisms within the electoral process.

One of **Marion's** most significant actions includes his vocal support for RLAs, which rely on meticulously organized ballot manifests and the integration of voter data into digital platforms. These audits, while marketed as tools to bolster election integrity, fundamentally compromise voter anonymity by embedding traceable data points within the audit process. **Marion's** involvement in advocating for such audits places him at the intersection of state and national efforts to redefine election security in ways that prioritize data centralization over constitutional protections for voter privacy.

Additionally, **Marion's** connection to **Common Cause's** broader national efforts cannot be overlooked. **Common Cause,** as part of a larger network of advocacy organizations, has received funding from entities tied to **Microsoft, Democracy Fund,** and other major players in election technology. This funding supports initiatives that, while presented as democratic safeguards, **effectively consolidate power within a narrow group of stakeholders, including private vendors and federal agencies**. **Marion's** leadership role implicates him in the propagation of these initiatives, which align with the broader agenda to federalize and privatize election infrastructure under the guise of securing it against foreign interference.

Marion's specific culpability lies in his apparent lack of opposition to the systemic vulnerabilities introduced by these reforms. As someone deeply embedded in **Rhode Island's** political advocacy landscape, he is uniquely positioned to understand the implications of centralized data storage, cloud-based voter systems, and the erosion of traditional state-level autonomy in election administration. His failure to address these

issues—or worse, his active promotion of policies that exacerbate them—raises questions about his motivations and the extent of his alignment with national organizations driving these changes.

Furthermore, **Marion's** public statements about combating election disinformation and promoting transparency ring hollow when juxtaposed with his support for policies that obscure the very systems he claims to defend. The reliance on RLAs, combined with centralized voter databases and data-sharing agreements with federal entities, creates a framework that enables surveillance-like capabilities under the pretense of enhancing voter confidence. **Marion's** role in advancing these measures positions him not as a defender of democracy but as a participant in its incremental erosion.

In examining **Marion's** actions through the lens of this investigation, it becomes clear that his contributions to **Rhode Island's** election reforms are emblematic of a larger national strategy to reframe election security. This strategy, driven by private vendors, federal advisory agencies, and advocacy organizations, seeks to integrate state systems into a centralized architecture that prioritizes control over transparency. **Marion's** involvement, whether intentional or not, makes him complicit in the broader scheme to undermine the constitutional safeguards designed to protect voter anonymity and electoral integrity. His career and actions, therefore, must be scrutinized not only for their local impact but also for their role in advancing a national agenda that prioritizes systemic control over democratic principles.



MATT MASTERSON

Senior Cybersecurity Advisor,
Department of Homeland Security

Matthew Masterson is the Senior Cybersecurity Advisor for the Department of Homeland Security. Previously, Masterson served as the chairman of the U.S. Election Assistance Commission from 2014 to 2018. Masterson previously held various positions within the Ohio secretary of state's office, where he managed voting system certification procedures and led the development of online voter registry and ballot delivery platforms for military and overseas voters.

Matt Masterson serves as a pivotal figure in connecting the **federal government**, **state election directors**, and **private cybersecurity companies** such as **CrowdStrike,** solidifying his role as an ***architect of the centralized election system infrastructure*** currently under investigation. His career spans critical positions that directly facilitated

the integration of Risk-Limiting Audits (RLAs), federal oversight of elections through the **DHS** and **CISA**, and the controversial partnerships with private companies such as **CrowdStrike**, which is fraught with vulnerabilities and accountability issues outlined extensively in **Volume 3** of this investigation.

Masterson's role at the **DHS** as **Senior Cybersecurity Advisor** during the height of election system centralization efforts placed him at the **nexus of policy, strategy, and operational decisions**. As a leader in the #**Protect2020 initiative**, he advocated for the ***federal designation of election infrastructure as critical infrastructure***, effectively paving the way for increased federal control and oversight under the pretext of cybersecurity. ***This designation was leveraged to justify the involvement of federal agencies like CISA, DHS, and the EI-ISAC/MS-ISAC in the management and monitoring of election systems, thus eroding the independence of state-run elections.***

Masterson's advocacy for RLAs, positioned as tools to enhance transparency and voter confidence, became a vehicle for centralizing election data through ***detailed ballot manifests, digital tracking, and cross-agency information sharing***. Under his leadership, these systems prioritized centralized control over voter privacy, enabling mechanisms that can re-link voter identities to ballots. His deliberate promotion of these frameworks highlights a prioritization of centralized oversight and federal influence over decentralized election protections.

The integration of private companies like **CrowdStrike** into election security further underscores **Masterson's** role in embedding known vulnerabilities into the system. Despite **CrowdStrike's** widely documented security flaws, including those in its **Falcon platform** detailed in **Volume 3, Masterson** facilitated its significant involvement in the election security framework. His willingness to embed these vendors, despite their failings, raises critical concerns about the priorities and motivations behind his decisions.

Masterson's influence extended to state election officials through his roles at the **EAC** and **NASED**, where he was instrumental in shaping state adoption of federally aligned practices. His collaboration with **Stuart Holmes** in **Washington** exemplifies this influence. **Holmes**, as a key figure in implementing **Washington's VoteWA** system, relied on **Masterson's** guidance to align state election systems with federally promoted practices like Risk-Limiting Audits (RLAs). ***Masterson's advocacy ensured that Holmes and other state officials adopted centralized frameworks that integrated***

cloud-based systems, such as Microsoft Azure, into the state's election infrastructure. This partnership not only standardized data-sharing agreements but also facilitated the monitoring and cross-referencing of election data at a federal level. Masterson's coordination with Holmes highlights his active role in embedding these systems, effectively dismantling the decentralized structure of U.S. elections and increasing federal oversight under the guise of enhanced security.

The establishment of data-sharing agreements between state election systems and federal entities, facilitated by **Masterson**, further demonstrates his culpability. ***These agreements enabled sensitive voter data and election infrastructure information to flow into centralized platforms like Microsoft Azure, where it could be queried and cross-referenced. The evidence underscores his knowledge of the implications of such systems, which undermine voter anonymity and constitutional protections while facilitating federal overreach into state election sovereignty.***

Masterson's leadership in initiatives like "Tabletop the Vote" exercises reveals his efforts to align state election directors with federal strategies under the guise of preparing for election day disruptions. While framed as security preparedness, these exercises conditioned state officials to view federal involvement as indispensable, embedding federal oversight into election management at all levels.

His failure to enforce compliance with federally mandated cybersecurity standards, such as those outlined in **EO 13800**, further illustrates the depth of his negligence. As **Senior Cybersecurity Advisor, Masterson** was uniquely positioned to ensure adherence to these requirements. Instead, he prioritized RLAs and centralized frameworks, neglecting the critical need for pre-election compliance testing and third-party assessments. This systemic negligence compromised election security and undermined the integrity of the critical infrastructure designation itself.

Masterson's expansive influence and deliberate choices reflect a calculated effort to centralize control over election systems, prioritize operational frameworks over legal obligations, and embed vulnerabilities into the electoral infrastructure. ***His actions have eroded voter privacy, weakened state autonomy, and facilitated federal overreach, leaving the U.S. election system exposed to manipulation and exploitation***. **Masterson's** role demands accountability, as his leadership has directly contributed to the systemic vulnerabilities now entrenched in the electoral process.



JENNIFER MORRELL

Consultant & Former Election Official

Jennifer Morrell works as a consultant with Democracy Fund leading the Election Validation Project, aimed at increasing trust in elections through rigorous audits, standards, and testing. As the Deputy of Elections in Arapahoe County, Colorado, Jennifer was instrumental in Colorado's successful implementation of the first statewide risk-limiting audit. She has a vision of creating uniform audit and testing standards for all critical components of the election system. Jennifer worked as an election official for nine years (2009-2018) in Utah and Colorado. She is an Election Center CERA graduate and holds a Master of Arts in Management from Webster University.

Jennifer Morrell represents a pivotal figure in the development and promotion of Risk-Limiting Audits (RLAs) as the foundation of modern election auditing practices. Her role as a **CISA Election Security Expert Consultant** and her deep involvement with **The Elections Group** have positioned her as a ***central architect*** of the auditing systems that now dominate the election security landscape. However, her actions and omissions raise critical concerns about the prioritization of centralized frameworks, the neglect of federally mandated cybersecurity standards, and the erosion of voter privacy under the guise of election security.

Jennifer Morrell has consistently championed RLAs, portraying them as the gold standard for election auditing. Her contributions include authoring guidance documents, conducting workshops, and speaking at conferences to promote RLAs as the optimal solution for ensuring election accuracy and transparency. These efforts have embedded RLAs into state election systems across the country, with **Morrell** frequently positioned as the trusted voice educating officials on their implementation. ***Her training materials emphasize detailed ballot manifests, voter registration audits, and digital systems integration—elements that are portrayed as enhancing accountability but that, in practice, introduce significant risks.***

RLAs, as promoted by **Morrell**, rely on detailed ballot tracking and centralized storage systems, such as **Microsoft Azure**, to maintain order and organization during audits. These mechanisms, while operationally efficient, conflict with constitutional mandates for voter anonymity. ***By enabling digital imprinting and systematic organization of ballots and envelopes, RLAs allow for the re-linking of ballots to individual voters, undermining fundamental privacy protections.*** While **Morrell** and her advocates claim

that these systems separate voter identities from ballots, the implementation of RLAs—especially when combined with centralized cloud storage—creates a framework that facilitates the opposite. This duality between operational efficiency and privacy erosion is a recurring theme in **Morrell's** work.

Morrell's collaboration with **The Elections Group** underscores her alignment with private interests that benefit from centralized election oversight. This organization partners with **state and local election officials** to implement audit frameworks and integrate proprietary tools and software into election systems. By promoting these frameworks, **Morrell** has facilitated the adoption of centralized systems that prioritize control and accessibility of election data over voter privacy. Her involvement with **The Elections Group** demonstrates her influence in embedding these practices into **state and local election protocols**, further consolidating data and oversight into centralized frameworks.

Jennifer Morrell's influence extends beyond RLAs and into broader election management practices. ***She has authored materials and provided training on voter registration database audits, GIS tools for district assignments, and ballot reconciliation procedures.*** These contributions reflect her technical expertise and comprehensive understanding of election infrastructure. ***However, her training efforts fail to address the critical need for compliance testing with federally mandated cybersecurity standards, as required for critical infrastructure under Executive Order 13800.*** Her omission of this critical component leaves election systems vulnerable to cyber threats, despite the operational improvements her frameworks aim to provide.

Her participation in **federal and state-level forums** highlights her ability to shape both technical practices and public narratives. Through her involvement with **CISA**, **Morrell** has taken an active role in combating misinformation and disinformation in elections. Her focus on managing narratives positions her as a key player in controlling the public perception of election security. However, this narrative control also allows for the dismissal of legitimate concerns about the centralized frameworks she promotes. Her ability to frame RLAs and centralized auditing systems as essential to election integrity effectively normalizes their adoption while obscuring their risks.

Jennifer Morrell's collaboration with figures like David Becker of ERIC and organizations like the Center for Internet Security (CIS) cements her place within a tightly interconnected network of stakeholders that prioritize centralized data sharing

and control. Her advocacy for RLAs aligns with the goals of these groups, which include **aggregating voter data across jurisdictions and facilitating real-time election monitoring capabilities**. These practices, while ostensibly aimed at improving coordination and security, create significant privacy concerns. ***The systems Morrell promotes depend on data-sharing agreements and centralized storage solutions that inherently expose sensitive voter information to potential misuse.***

Her extensive connections and deep technical knowledge reveal her as fully aware of the implications of the systems she advocates. As a former election official with hands-on experience, **Morrell** understands the vulnerabilities introduced by RLAs and centralized systems. Her decision to prioritize operational frameworks over privacy protections and compliance testing demonstrates a deliberate alignment with centralized control agendas. This alignment, combined with her federal and private sector connections, raises serious questions about her motivations and the broader impact of her work.

By framing RLAs as the cornerstone of election auditing, **Jennifer Morrell** has fundamentally reshaped how elections are managed and secured. Her advocacy has facilitated the erosion of voter privacy, the centralization of election data, and the neglect of federally mandated cybersecurity standards. Through her training programs, collaborations, and public engagements, **Morrell** has normalized systems that prioritize control and data centralization, leaving election systems increasingly dependent on frameworks that compromise foundational principles of transparency and sovereignty.

Jennifer Morrell's role in modernizing election auditing practices cannot be understated. However, her neglect of critical cybersecurity requirements, combined with her promotion of centralized frameworks, positions her as a key contributor to systemic vulnerabilities in election infrastructure. Her actions reflect a deliberate choice to prioritize operational efficiency and narrative control over the legal and ethical obligations that should guide election security practices. As one of the ***primary architects*** of RLAs and centralized election systems, **Morrell's** influence demands accountability and critical examination within the broader context of election security.



KELLIE OTTOBONI

Ph.D Candidate in Statistics, UC Berkeley

Kellie is a Ph.D candidate and fellow at the Berkeley Institute for Data Science doing statistics for social good. Her research interests include nonparametrics, inference, reproducibility and open science, and election integrity.

Kellie Ottoboni represents a significant figure in the development and operationalization of Risk-Limiting Audits (RLAs), particularly through her academic research and practical applications in election security. Her background as a statistician and data scientist has positioned her as a technical authority in the methodologies that underpin RLAs. Working closely with institutions like the **University of California, Berkeley**, under the mentorship of **Philip B. Stark, Ottoboni's** contributions have helped shape the statistical foundations that make RLAs operationally viable, while also embedding vulnerabilities into their framework under the guise of efficiency.

Ottoboni's research and development efforts include co-authoring critical works on statistical techniques that refine how RLAs are conducted, such as the SUITE (Stratified Union-Intersection Tests of Elections) method. This methodology, promoted as a way to enhance the accuracy and efficiency of audits, requires granular ballot manifest data and relies on statistical stratification to justify lower sampling thresholds. ***While technically advanced, these techniques prioritize centralized control and digital infrastructure, introducing inherent risks. Her insistence on the granular organization of ballots and their metadata for stratified sampling directly feeds into the systemic issues of centralized storage and traceability, undermining voter anonymity and constitutional protections.***

Her involvement in **Michigan's** first RLA pilot in 2018 exemplifies her practical impact. **Ottoboni** worked closely with state and local election officials to design and implement post-election audit procedures that relied heavily on digital tools for ballot tracking and statistical verification. By embedding these processes into state systems, she played a key role in normalizing the data collection and centralization practices that RLAs require. These pilots not only paved the way for widespread adoption of RLAs but also revealed the underlying risks associated with their implementation, including the ability for re-linking voter identities to ballots through metadata and digital imprints.

Ottoboni's collaboration with figures like **Philip B. Stark** and other key RLA architects situates her within a network of statisticians and election security advocates who are deeply embedded in the federal and state election oversight ecosystem. Her statistical methodologies are foundational to the frameworks adopted by federal agencies and state election directors, yet her work also intersects with private vendors and software platforms that facilitate the centralized election management systems criticized for their vulnerabilities.

After investigating **Ottoboni's** connections, her culpability in promoting centralized election oversight becomes evident. Her methodologies rely on the very infrastructures —such as detailed ballot manifests and cloud-based storage solutions—that create systemic vulnerabilities. By focusing on statistical optimization, **Ottoboni** has contributed to the erosion of decentralized election protections and the increased dependency on digital tools that prioritize operational convenience over voter privacy.

The connection to **Matt Bernhard** further underscores the broader network in which **Ottoboni** operates. **Bernhard**, a fellow statistician and election security advocate, shares significant overlap with **Ottoboni** in both methodology and application. His work, as detailed in the provided files, delves into the technical specifics of digital infrastructure, ballot metadata, and security protocols that align closely with **Ottoboni's** contributions.

In analyzing the **"Matt Bernhard"** files, it becomes clear that his research provides the technical underpinnings that complement **Ottoboni's** statistical approaches. His dissertation and related works discuss the security flaws in electronic voting systems and their integration with post-election audits. **Bernhard's** focus on system vulnerabilities and the technical frameworks for ballot tracking aligns with **Ottoboni's** statistical methodologies, creating a seamless integration of technical and operational strategies for RLAs.

For example, **Bernhard's** research highlights how digital ballot imprints and metadata can be used for stratified sampling, a process **Ottoboni** champions. However, his work also exposes the inherent risks of these practices, particularly their potential for misuse in re-linking voter identities to ballots. This overlap reveals a collaborative effort to design and promote systems that, while technically robust, embed risks that are not adequately addressed in their frameworks. The shared focus on digital infrastructure and

metadata management between **Ottoboni** and **Bernhard** reflects a coordinated effort to centralize election management under the guise of statistical and technical optimization.

The ***"Survey Statewide RLA"*** document further illustrates **Ottoboni's** involvement in scaling these methodologies to a national level. ***Her statistical techniques are embedded in the survey's recommendations, which emphasize the necessity of detailed ballot manifests and digital infrastructure for statewide audit implementation.*** This approach not only reinforces centralized data practices but also aligns with **Bernhard's** technical frameworks, demonstrating their joint influence on national election security standards.

Kellie Ottoboni's work represents a critical juncture between statistical innovation and the systemic vulnerabilities introduced by centralized election systems. Her collaboration with **Matt Bernhard** and others has created a network of methodologies and technical frameworks that prioritize efficiency and control at the expense of privacy and constitutional protections. Their combined contributions have facilitated the adoption of RLAs on a national scale, embedding systems that compromise voter anonymity and introduce significant risks under the pretext of enhancing election integrity. **Ottoboni's** role, while framed as technical and statistical, is deeply intertwined with the broader agenda of centralizing election oversight, making her a pivotal figure in the ongoing transformation of U.S. election systems.

Matt Bernhard's contributions to the election security landscape are deeply rooted in his technical expertise and focus on the vulnerabilities inherent in electronic voting systems and post-election audit frameworks. His dissertation and associated works offer a meticulous examination of how digital infrastructures interact with the operational mechanics of elections, particularly in the context of RLAs.

Bernhard's research emphasizes the technical mechanisms that underpin modern election systems, including the use of digital ballot imprints and metadata for tracking and verification. His analysis highlights the dual-edged nature of these technologies: while they provide a pathway for stratified sampling and audit precision, they also open doors to misuse. **Bernhard's** work meticulously documents how these systems create digital trails that, if improperly managed, allow for the re-linking of voter identities to their ballots. This revelation underscores a critical flaw in the RLA framework—a vulnerability that is not just theoretical but actively embedded in the systems being promoted.

His detailed exploration of electronic voting machines delves into their susceptibility to external manipulation, including software vulnerabilities and hardware exploitation. **Bernhard** identifies specific attack vectors that could compromise the integrity of election results, particularly in systems reliant on centralized data storage. This research not only reinforces the risks posed by electronic voting but also draws direct connections to the infrastructures championed by figures like **Ottoboni**. Their combined work effectively lays the groundwork for election management systems that, while operationally efficient, embed systemic risks that are difficult to mitigate.

The **"Matt Bernhard"** files further reveal his involvement in developing technical solutions aimed at enhancing audit processes, such as improved methods for ballot tracking and metadata management. However, these solutions also perpetuate the reliance on centralized infrastructures that inherently conflict with voter privacy principles. **Bernhard's** advocacy for these methods reflects a broader alignment with the centralized election oversight frameworks promoted by **Ottoboni** and others, demonstrating a shared agenda to embed these practices into national standards.

Matt Bernhard's work provides the technical scaffolding for the statistical methodologies advanced by **Kellie Ottoboni** and others. His research bridges the gap between operational theory and technical implementation, revealing both the potential and the risks of the systems he champions. While his contributions underscore the sophistication of modern election auditing techniques, they also highlight the systemic vulnerabilities and privacy concerns that accompany their widespread adoption. Together, **Bernhard** and **Ottoboni** represent a coordinated effort to redefine election security through centralized control, raising critical questions about the trade-offs between efficiency, transparency, and constitutional protections.



DR. RONALD L. RIVEST

Institute Professor, MIT

Professor Rivest is an Institute Professor at MIT. He joined MIT in 1974 as a faculty member in the Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory, a member of the lab's Theory of Computation Group, and a founder of its Cryptography and Information Security Group. He is a co-author of the text, Introduction to Algorithms. He is also a founder of RSA Security, Versign, and Peppercoin.

Dr. Ronald L. Rivest emerges as a towering figure in the intersection of cryptographic methodologies, election security, and computational advancements, serving as one of the pivotal architects in shaping modern secure voting systems. As an **Institute Professor at the Massachusetts Institute of Technology (MIT), Rivest's** foundational contributions to cryptography, such as the co-creation of the RSA encryption algorithm, have established him as a cornerstone in the field of secure communications. His transition into election security was a natural extension of his expertise, and he has since become a vital voice in advocating for the integration of **end-to-end verifiable (E2E-V)** systems and Risk-Limiting Audits (RLAs) into the U.S. electoral process.

Rivest's work emphasizes creating robust election infrastructures that blend advanced cryptographic solutions with transparent audit mechanisms. His participation in committees like the **National Academies' *"Securing the Vote: Protecting American Democracy"* initiative** and other high-level collaborations underscores his influence in shaping the national conversation on electoral security. **Rivest** has contributed to designing protocols that aim to provide end-to-end verifiability, a principle that ensures voters and officials can verify every step of the electoral process, from vote casting to tabulation.

A notable focus of **Rivest's** contributions lies in RLAs, a statistical auditing method designed to detect and correct discrepancies in election outcomes. RLAs provide mathematical guarantees about the accuracy of election results, relying on secure sampling and verification techniques. His expertise in designing cryptographic safeguards is directly applied to enhancing these audits, ensuring they remain resistant to manipulation while preserving voter privacy.

The uploaded documents provide further insights into **Rivest's** contributions. For instance, his co-authored works in ***"Securing the Vote"*** lay out comprehensive recommendations for strengthening electoral systems. These include advocating for human-readable paper ballots, the adoption of robust audit systems, and rigorous cybersecurity protocols. **Rivest's** push for the adoption of **E2E-V** systems reflects his belief in the necessity of transparent and verifiable election mechanisms, which align closely with his cryptographic principles.

In the article ***"Going From Bad to Worse,"*** **Rivest** delves into vulnerabilities in electronic voting systems, particularly the potential for cascading failures when insecure voting mechanisms are integrated without sufficient safeguards. His analysis highlights

the dangers of relying on proprietary systems without independent oversight, a critique that resonates with broader concerns about centralization and privatization in election management.

Dr. Rivest's culpability lies not in negligence but in the broader implications of the systems he champions. While his designs aim to enhance security and transparency, their implementation often intersects with centralized frameworks that introduce risks to voter privacy and election autonomy. His role in promoting **E2E-V** and RLAs underscores a tension between technical innovation and systemic vulnerabilities, particularly when these methods are deployed within existing insecure infrastructures.

Rivest's influence extends beyond academia into policy and operational realms, where his cryptographic frameworks shape both the technical and strategic dimensions of election security. His collaboration with other high-profile figures in the election security ecosystem situates him as a key player in advocating for centralized auditing and verification methods. While these methods promise increased accuracy and transparency, they also consolidate control over electoral processes, raising concerns about oversight and accountability.

Dr. Ronald L. Rivest embodies the dual-edged sword of technological innovation in election security. His work, while groundbreaking, underscores the complexities of integrating advanced cryptographic methods into a fractured and vulnerable electoral infrastructure. As a thought leader and architect of secure voting methodologies, **Rivest's** contributions are instrumental in shaping the future of electoral integrity, but they also necessitate critical scrutiny to ensure their deployment aligns with constitutional protections and voter autonomy.

The book "***Securing the Vote: Protecting American Democracy"*** sets out to establish itself as the definitive guide to election security reform in the wake of mounting concerns over the vulnerabilities of the United States' electoral systems. Authored by a panel of esteemed academics, technologists, and institutional leaders, including **Dr. Ronald L. Rivest,** its publication aligns with growing national anxiety about foreign interference, systemic weaknesses in voting technology, and the erosion of public confidence in democratic processes. Framed as an unbiased, solutions-oriented analysis, the book argues for transformative changes in election security infrastructure, leaning heavily on statistical tools like Risk-Limiting Audits (RLAs) and centralized

technological solutions. However, beneath its veneer of academic rigor lies a more troubling narrative.

The panel, chaired by **Dr. Lee Bollinger of Columbia University** and **Dr. Michael McRobbie of Indiana University,** represents the intellectual elite of the election reform movement. Their expertise in cryptography, public policy, and computer science lends weight to their recommendations, but it also reveals the extent to which high-level academic and institutional leaders have been complicit in advancing an agenda that prioritizes centralization and control over transparency and constitutional protections. These authors, heralded as impartial stewards of democracy, are instrumental in normalizing systems that systematically compromise voter anonymity and weaken the decentralization historically critical to U.S. elections.

The authors situate their analysis against a backdrop of rising foreign cyber threats, drawing from the fallout of the 2016 U.S. presidential election. They emphasize the dual imperatives of technical accuracy and public trust, suggesting that only sweeping reforms can restore confidence in the electoral process. Yet, their focus on public trust seems more rhetorical than substantive, as their proposed solutions directly undermine the safeguards of voter privacy and state sovereignty enshrined in U.S. constitutional and electoral law. ***The very experts who outline the vulnerabilities of decentralized systems use this critique to justify an intrusive federal role in elections, facilitated by partnerships with private vendors like Microsoft and CrowdStrike.***

The book identifies the decentralized nature of U.S. elections as both a strength and a weakness. While decentralization prevents the systemic failures that can plague monolithic systems, it also allows significant disparities in security practices between jurisdictions. The authors lean on these disparities to advocate for uniform standards and greater federal oversight, overlooking the constitutional principle that elections are primarily a state responsibility. Their emphasis on centralization runs counter to the very diversity and independence that provide resilience against cyberattacks. By proposing that vulnerabilities in one jurisdiction necessitate federal interventions across all jurisdictions, the authors frame decentralization as a liability rather than a safeguard, creating a pretext for federal agencies like **DHS** and **CISA** to assert increasing influence over elections.

What makes this particularly egregious is the deliberate omission of federal mandates already in place to secure critical infrastructure, such as **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF).** By failing to address these requirements, the authors obscure the fact that the systems they champion, such as RLAs, are not compliant with the very cybersecurity standards designed to protect critical infrastructure. ***This omission is not incidental; it allows states to exempt cast vote records from public records requests, shielding the federal involvement and private vendor activities that drive these systems. The authors' failure to emphasize compliance with federal law, while pushing for centralized auditing processes, reveals a troubling agenda that prioritizes control over transparency.***

The intellectual elite behind this book claim to champion the principles of election integrity and transparency, yet their methodologies and recommendations directly contradict these ideals. RLAs, which the book describes as a cornerstone of secure elections, are portrayed as a means of verifying outcomes and building public trust. ***However, their implementation depends on granular ballot manifests and metadata that create a digital footprint linking voters to their ballots. This design feature fundamentally violates the right to anonymous voting, a cornerstone of both U.S. constitutional law and international human rights agreements such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.*** The authors either fail to recognize or deliberately obscure the chilling implications of this centralization, which not only compromises voter privacy but also opens the door to systemic manipulation by federal agencies and private vendors.

Their emphasis on public confidence also appears disingenuous when juxtaposed with their dismissal of federal overreach concerns. By framing RLAs and centralized technological solutions as necessary to combat cyber threats, the authors sidestep the broader implications of placing critical election data in centralized, cloud-based systems like **Microsoft Azure.** These systems are not only vulnerable to breaches but also subject to the data-sharing agreements facilitated by the **Department of Homeland Security (DHS) and its subsidiaries, CISA and the EI-ISAC.** The authors fail to account for the risks associated with ***allowing federal agencies to access, monitor, and potentially manipulate voter data under the pretext of election security.***

The book's framing also raises questions about the loyalty of its authors to the principles of decentralized, state-run elections. By consistently favoring federalized solutions and private vendor integration over state-led initiatives, the book aligns more closely with a

vision of centralized control than one of cooperative federalism. This alignment becomes especially problematic given the involvement of private companies like **CrowdStrike**, whose documented vulnerabilities in election systems were explored in **Volume 3** of this investigation. The authors' silence on these issues further underscores their complicity in advancing a centralized agenda that erodes voter sovereignty and electoral integrity.

Securing the Vote: Protecting American Democracy presents itself as a blueprint for election security reform but ultimately serves as an intellectual justification for centralizing control over U.S. elections. By prioritizing RLAs and federal oversight while neglecting existing legal frameworks and constitutional protections, the authors have laid the groundwork for a system that prioritizes control over transparency, efficiency over privacy, and federal dominance over state sovereignty. Far from securing the vote, the book's recommendations expose it to new vulnerabilities and diminish the foundational principles of democratic governance.

The book moves from a broad introduction into a deep dive on the vulnerabilities and perceived inadequacies of the United States' election infrastructure. It presents a picture of systemic fragility, painting decentralized election administration as both a significant weakness and a barrier to uniform security practices. This section critiques the current state of voting technology, voter registration databases, and cybersecurity practices while presenting a vision for what the authors frame as necessary modernization.

The authors highlight the inconsistent state of voting technology across the country, focusing on the prevalence of outdated voting machines, poorly maintained voter registration databases, and the lack of standardized cybersecurity protocols. They identify these shortcomings as major risks to election integrity, emphasizing that the fragmented nature of election administration leaves jurisdictions vulnerable to both targeted and opportunistic cyberattacks. These vulnerabilities, they argue, have been exploited or exposed in high-profile incidents, particularly during the 2016 election cycle. The authors contend that this decentralization complicates efforts to secure elections uniformly and opens the door to failures that could erode public confidence in the system.

On the surface, this critique seems to serve a pragmatic purpose: pointing out weaknesses and suggesting avenues for improvement. However, the solutions they propose are deeply problematic. Their vision of a modernized election system relies on a

centralized framework that fundamentally undermines the diversity and autonomy of state-run elections. By advocating for uniform standards and practices, the authors conflate security with centralization, disregarding the principle that decentralization serves as a critical safeguard against systemic failures and centralized tampering. While the book pays lip service to the idea of state and local control, its recommendations encourage the federal government to take on a more dominant role in managing election infrastructure.

The most glaring flaw in this analysis is its failure to address the existing federal mandates that already provide a framework for election security. **Executive Order 13800,** issued in 2017, requires all critical infrastructure—including election systems—to adopt the **NIST Cybersecurity Framework (CSF)** to ensure resilience against cyber threats. This mandate is designed to create a baseline of security without infringing on state autonomy. The authors' omission of this critical requirement from their discussion reveals a deliberate avoidance of addressing compliance failures at the state and federal levels. Instead of reinforcing these standards, the authors focus on implementing new measures—like Risk-Limiting Audits (RLAs)—that further entrench centralized data collection and oversight while bypassing existing cybersecurity requirements.

A critical element of the book's recommendations is the modernization of voter registration databases. The authors argue for the integration of advanced digital systems to streamline voter registration processes, improve accuracy, and enhance security. However, this integration requires centralized databases that inevitably link state systems with federal entities like **DHS** and **CISA**. While the authors emphasize the potential efficiency gains from such integration, they fail to address the risks posed by centralized storage of sensitive voter information, especially when these systems are subject to federal oversight and data-sharing agreements. The move toward centralization undercuts the protections offered by decentralized systems, which limit the scope of breaches and ensure that no single entity has comprehensive access to voter data.

The book's discussion of electronic voting machines is similarly flawed. The authors advocate for replacing outdated systems with modern, paper-based voting machines capable of producing voter-verifiable paper trails. While this recommendation aligns with best practices for election security, the authors' framing of this transition reveals a bias toward centralization. They argue that modern systems should be accompanied by standardized auditing practices, specifically RLAs, that rely on ***detailed ballot manifests***

and digital tracking. This approach introduces new vulnerabilities, as it creates opportunities for re-linking voter identities to their ballots through metadata and digital imprints. The authors' insistence on RLAs as a cornerstone of election integrity ignores the systemic risks they introduce, ***including violations of constitutional protections for anonymous voting***.

The authors also discuss the role of federal agencies and private vendors in securing election infrastructure. They highlight the need for collaboration between state and federal governments while advocating for partnerships with private companies to provide technical expertise. However, this framing glosses over the significant risks posed by these partnerships. Federal agencies like **DHS** and **CISA**, while ostensibly providing guidance, often leverage their involvement to assert control over state systems. Meanwhile, private vendors like **Microsoft** and **CrowdStrike**, which are deeply embedded in the election security ecosystem, introduce proprietary solutions that lack transparency and are riddled with vulnerabilities. The authors fail to critically assess the implications of these partnerships, instead portraying them as necessary components of a modernized election system.

By framing decentralization as a liability rather than a strength, the authors lay the groundwork for increased federal control and private sector influence over elections. This shift fundamentally alters the balance of power in the U.S. electoral system, moving it away from the decentralized, state-run model envisioned by the Constitution. The book's failure to address the legal and ethical implications of this shift, particularly in light of existing federal cybersecurity mandates, reveals a troubling alignment with the interests of federal agencies and private vendors over those of voters and state governments.

In critiquing the current state of election infrastructure, the authors of ***"Securing the Vote"*** reveal their preference for a centralized, federally controlled system. Their analysis, while technically accurate in identifying vulnerabilities, is strategically designed to justify interventions that undermine voter privacy, state sovereignty, and constitutional protections. Rather than addressing the root causes of these vulnerabilities —such as noncompliance with existing federal standards—the authors propose solutions that exacerbate systemic risks and concentrate power in ways that serve the interests of federal agencies and private companies. This approach not only fails to secure the vote but ***actively compromises the foundational principles of U.S. democracy.***

Risk-Limiting Audits (RLAs) take center stage in ***"Securing the Vote: Protecting American Democracy"*** as the authors position this statistical audit method as a cornerstone of election security. Their argument for RLAs is framed around the idea that these audits provide a statistically reliable means of verifying election outcomes, ensuring that the reported results align with the actual votes cast. The authors emphasize the purported benefits of RLAs—enhanced transparency, increased voter confidence, and the ability to detect and correct errors or fraud. However, a deeper examination reveals how RLAs, as presented in this book, serve as a tool for centralization and data aggregation under the guise of safeguarding electoral integrity.

The authors meticulously detail the mechanics of RLAs, explaining that the method relies on statistical sampling of ballots to determine whether a full recount would alter the election outcome. ***The process requires precise ballot manifests, which catalog each ballot's metadata, such as its batch, location, and order within the system. This level of granular data collection, while critical for the audit's statistical validity, introduces significant risks. The book largely avoids discussing how this data could be exploited to undermine voter anonymity, even though the very infrastructure required for RLAs makes such exploitation feasible.***

One of the book's most significant omissions is its failure to address how RLAs intersect with the constitutional and international legal protections for anonymous voting. By requiring **detailed ballot manifests**, RLAs create a framework where ballots can potentially be ***re-linked to individual voters, particularly when these manifests are stored alongside voter profiles in centralized databases. This is not a theoretical concern but a documented vulnerability in the systems promoted by federal agencies like CISA and private vendors such as Microsoft.*** The authors' silence on this issue is striking, given that voter anonymity is a cornerstone of democratic elections enshrined in both **U.S. constitutional law** and **international agreements like the Universal Declaration of Human Rights.**

The book also portrays RLAs as inherently neutral tools, overlooking the political and systemic implications of their adoption. The implementation of RLAs has been driven largely by federal agencies such as the **Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA),** and their associated **Information Sharing and Analysis Centers (EI-ISAC and MS-ISAC).** These agencies have leveraged their influence to embed these audits into state election systems under the pretense of enhancing security and transparency. In collaboration with private

sector partners such as **Microsoft**, which provides **Azure cloud infrastructure** for storing and analyzing election data; **Amazon Web Services (AWS),** a critical provider of cloud hosting for election-related systems; **CrowdStrike**, responsible for endpoint security despite its known software vulnerabilities; **Dominion Voting Systems**, whose proprietary machines play a central role in ballot tabulation; and **Clear Ballot**, which develops audit and verification software integral to RLAs, these efforts have created a framework that centralizes control over voter data and election processes. The authors fail to critique how this federal involvement, combined with the reliance on private vendors with significant security flaws and conflicts of interest, compromises state sovereignty over elections. Instead, they frame RLAs as a best practice that states should adopt to demonstrate their commitment to transparency. This framing ignores the broader agenda behind RLAs, which includes the centralization of voter data, increased federal oversight, and the ***erosion of state control over election administration.***

Furthermore, the authors' advocacy for RLAs sidesteps the compliance requirements outlined in **Executive Order 13800** and the **NIST Cybersecurity Framework (NIST CSF).** The infrastructure necessary for RLAs—digital ballot tracking systems, centralized data storage, and metadata management—is subject to federal cybersecurity standards. Yet the book does not discuss the need for these systems to undergo regular compliance testing or third-party audits, as mandated by **EO 13800**. This omission allows states to implement RLAs without addressing the underlying cybersecurity vulnerabilities that could compromise the entire electoral process. By failing to emphasize these requirements, the authors enable the proliferation of systems that are neither secure nor legally compliant.

The operational challenges of RLAs are another area where the book falls short. While the authors highlight the statistical rigor of RLAs, they downplay the practical difficulties of implementing these audits at scale. RLAs require significant investments in technology, training, and administrative resources, which many jurisdictions are ill-equipped to provide. The reliance on proprietary software and systems for conducting RLAs further complicates their adoption, creating dependencies on private vendors that limit transparency and accountability. ***The authors' lack of critical analysis regarding these challenges suggests either a willful ignorance or a deliberate attempt to obscure the systemic flaws inherent in their recommendations.***

Once again, the book's discussion of RLAs fails to address how these audits have been used to justify other forms of centralization, such as the integration of state election

systems with federal databases and cloud-based platforms. RLAs are presented as standalone solutions, but in practice, their implementation often requires states to adopt broader systems of data sharing and digital infrastructure. This creates a feedback loop where states become increasingly reliant on federal guidance and private vendors to manage their election systems, further eroding their independence.

The authors' portrayal of RLAs as a panacea for election security also raises questions about their broader motivations. While RLAs do offer a statistical means of verifying election outcomes, their adoption must be weighed against the systemic risks they introduce. By failing to engage with these risks, the authors contribute to a narrative that prioritizes operational convenience and centralized oversight over voter privacy and constitutional protections. ***This narrative aligns with the interests of federal agencies and private sector stakeholders, which stand to benefit from the centralization of election systems.***

The book's treatment of Risk-Limiting Audits exemplifies its broader approach to election security—technically sophisticated but strategically aligned with an agenda of centralization and control. RLAs, as described in ***"Securing the Vote",*** are not just tools for verifying election outcomes; they are mechanisms for embedding centralized data practices and federal oversight into state election systems. By championing RLAs without addressing their systemic flaws and legal implications, the authors undermine the very principles of transparency and accountability they claim to uphold. Their advocacy for RLAs reflects a calculated effort to reshape the U.S. electoral system in ways that compromise its foundational principles, ***raising serious questions about their loyalty to the ideals of democracy and voter sovereignty.***

The book transitions from its discussion of election infrastructure and RLAs to a detailed exploration of policy and governance recommendations, emphasizing the need for collaboration between federal, state, and local entities. At its core, this section argues that securing elections requires not only technical innovation but also a **reimagining of the roles and responsibilities of various stakeholders**. The authors present a roadmap for policy reforms that they claim will enhance election integrity, focusing on issues like standardizing best practices, strengthening federal oversight, and fostering public-private partnerships. While these proposals are framed as necessary steps toward a secure electoral system, their implications reveal a deeper agenda that prioritizes centralization and control over constitutional protections and state autonomy.

The authors' recommendations include the establishment of federal standards for voting technology and cybersecurity, which they argue would address the disparities in security practices across states. They propose that federal agencies, particularly **DHS** and **CISA**, take on a more prominent role in coordinating these efforts. ***This includes providing states with technical assistance, funding for modernization, and guidance on implementing post-election audits and data-sharing agreements***. At first glance, these suggestions appear pragmatic, especially given the well-documented vulnerabilities in outdated voting systems. ***However, they also signify a fundamental shift in the balance of power, with federal agencies exerting unprecedented influence over state-administered elections.***

The authors further advocate for the integration of public-private partnerships as a means of enhancing election security. They highlight the role of private vendors like **Microsoft, CrowdStrike,** and **Dominion** in providing technical expertise and innovative solutions. However, this reliance on private companies introduces significant risks. These vendors often operate with little transparency and accountability, using proprietary systems that shield their processes from public scrutiny. States have created their own election security compliance matrix, that gives vendors the ability to **"self-assess"** their compliance and does not even mention the federal requirements that they must conform to the standards set in the **NIST CSF** per **EO 13800**. By endorsing these partnerships without addressing their inherent vulnerabilities, the authors ignore the systemic risks posed by outsourcing critical election functions to entities with conflicting interests.

The book calling for increased information sharing between federal and state entities to combat misinformation, disinformation, and cyber threats should not be overlooked. While this may seem like a logical approach to safeguarding elections, it effectively institutionalizes the flow of sensitive voter data and election information into centralized platforms controlled by federal agencies and their private sector partners. The authors' failure to critique the implications of this data centralization is striking, given its potential to undermine voter privacy and state sovereignty. ***By framing information sharing as a collaborative necessity, the book glosses over the reality that these agreements often come with strings attached, granting federal agencies significant access to and control over state election systems.***

The book also emphasizes the need for improved training and **capacity-building programs** for **election officials**, recommending that federal agencies like **CISA** lead

these efforts. While training is undoubtedly important, the authors' framing of this recommendation reveals their intent to align state election officials with federally dictated practices. This approach effectively conditions state officials to view federal oversight as indispensable, further eroding the decentralized protections historically integral to U.S. elections. The authors do not address the potential for this alignment to create dependencies that limit states' ability to assert their independence in election administration.

A critical omission in this section is the lack of discussion about existing federal laws and standards, particularly Executive Order 13800 and the NIST Cybersecurity Framework (CSF). ***The book presents its recommendations as though they fill a void in election security policy, ignoring the fact that comprehensive cybersecurity standards for critical infrastructure already exist.*** By failing to emphasize the need for compliance with these mandates, the authors enable states and private vendors to **sidestep their legal obligations**. This omission raises questions about whether the authors' recommendations are truly aimed at enhancing security or merely facilitating the adoption of centralized systems under the guise of modernization.

The authors also fail to address the broader implications of their recommendations on voter anonymity and constitutional protections. Their proposals often rely on digital infrastructure and centralized data systems that compromise these principles. For example, the emphasis on standardizing voter registration databases and integrating them with federal systems introduces vulnerabilities that allow for the re-linking of voter identities to their ballots for bad actors with access. This risk is compounded by the reliance on private vendors, whose systems often lack the transparency necessary to ensure that voter data is handled securely and ethically.

In critiquing these policy recommendations, it becomes clear that the authors' vision for election security aligns more closely with the interests of federal agencies and private vendors than with the principles of state sovereignty and voter privacy. By framing centralization as a necessity and downplaying the systemic risks it introduces, the authors advance an agenda that prioritizes control over accountability. Their failure to engage with existing legal frameworks and their selective focus on certain vulnerabilities suggest a deliberate strategy to reshape the U.S. electoral system in ways that benefit centralized authorities at the expense of democratic principles.

The policy and governance recommendations in ***"Securing the Vote"*** reflect a calculated effort to normalize federal and private sector control over elections. While the authors claim to prioritize security and transparency, their proposals often undermine these very principles by enabling the centralization of power and data. Their vision for election reform, though presented as a solution to existing vulnerabilities, raises significant concerns about its impact on voter privacy, state sovereignty, and the integrity of the democratic process. This section of the book, like the rest, must be viewed critically as part of a broader effort to consolidate control over the electoral system under the pretext of modernization and security.

The book delves into the role of technology and innovation in modernizing election systems, presenting technological advancements as both an opportunity and a challenge. The authors emphasize the transformative potential of emerging tools like blockchain voting, electronic poll books, and end-to-end verifiable voting systems. They argue that these technologies could revolutionize the electoral process by making voting more accessible, secure, and efficient. However, they acknowledge that the adoption of these tools must be accompanied by rigorous security measures to mitigate risks.

While the authors' optimism about technological innovation is evident, their discussion often lacks the critical analysis necessary to address the systemic vulnerabilities introduced by these technologies. For example, their endorsement of blockchain voting as a potential solution to issues of trust and transparency fails to grapple with the broader implications of integrating such a system into the existing election infrastructure. Blockchain systems, while decentralized in theory, require a high degree of technical expertise and centralized oversight in practice. The authors downplay the risks of data breaches, software vulnerabilities, and the potential for misuse by federal agencies or private entities with access to these systems.

The book's treatment of electronic poll books is similarly problematic. The authors present these tools as an efficient alternative to traditional voter rolls, capable of streamlining the check-in process and reducing errors. However, electronic poll books rely heavily on centralized databases and digital infrastructure, which are inherently vulnerable to cyberattacks. The authors fail to address how these vulnerabilities could be exploited to disrupt elections or manipulate voter data. Additionally, they overlook the implications of integrating these systems with state and federal databases, which could enable real-time tracking of voter participation and compromise voter anonymity.

End-to-end verifiable voting systems are another area where the book's analysis falls short. These systems are designed to allow voters to confirm that their votes were cast and counted as intended without revealing how they voted. While the concept aligns with the principles of transparency and voter confidence, the implementation of these systems often requires detailed digital tracking and metadata collection. The authors do not sufficiently critique how these features could be exploited to undermine voter anonymity, particularly when combined with centralized data storage solutions like **Microsoft Azure** or **Amazon Web Services**. By focusing on the theoretical benefits of these technologies, the book glosses over their real-world risks and the broader implications for voter privacy and election security.

A critical oversight in this section is the lack of discussion about compliance with federal cybersecurity standards. Technologies like blockchain, electronic poll books, and verifiable voting systems must adhere to the requirements outlined in **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF).** The book's failure to address these legal obligations allows it to present these tools as panaceas without acknowledging the systemic vulnerabilities they introduce when implemented outside the framework of federal law. This omission is particularly troubling given the authors' emphasis on modernizing election systems, which inherently requires adherence to established cybersecurity protocols.

The authors also fail to adequately address the role of private vendors in developing and deploying these technologies. Companies like **Microsoft, Amazon, Dominion,** and **Clear Ballot** are deeply involved in the design and operation of these systems, often using proprietary software that shields their processes from public scrutiny. The reliance on these vendors creates dependencies that limit transparency and accountability, yet the book portrays their involvement as a necessary partnership rather than a systemic risk. By endorsing these partnerships without critical analysis, the authors contribute to a narrative that normalizes private sector control over critical election functions.

Moreover, the book's discussion of technology and innovation lacks a meaningful critique of the centralization that these tools necessitate. While the authors acknowledge the risks of cyberattacks and data breaches, they do not fully explore how centralized systems increase these vulnerabilities. Centralized databases, cloud storage solutions, and digital tracking systems concentrate sensitive voter data in ways that make them attractive targets for exploitation. The authors' failure to engage with these risks reveals

a bias toward centralization that aligns with the broader agenda of federal control over elections.

The book's exploration of technology and innovation reflects its broader approach to election security: an emphasis on theoretical benefits without sufficient consideration of practical risks and systemic implications. While the authors present emerging technologies as solutions to the challenges facing election systems, their analysis often overlooks the vulnerabilities these tools introduce and the legal and ethical obligations they entail. By prioritizing operational efficiency and technological advancement over transparency, accountability, and voter privacy, the authors advance a vision of election modernization that ultimately compromises the foundational principles of democracy. This section, like others in the book, must be critically examined as part of a broader effort to centralize election oversight under the guise of innovation and security.

The concluding sections of ***"Securing the Vote: Protecting American Democracy"*** aim to synthesize the authors' analysis into actionable recommendations for policymakers, election officials, and other stakeholders. They advocate for a comprehensive strategy to secure elections, encompassing federal standards, technological modernization, enhanced audits, and collaborative partnerships between public and private sectors. While these proposals are framed as solutions to the vulnerabilities identified earlier in the book, they ultimately serve to reinforce the centralized framework that undermines the decentralized electoral protections foundational to American democracy.

The authors emphasize the need for robust federal standards to ensure uniformity in election security practices across states. They argue that such standards are necessary to address disparities in cybersecurity preparedness and technological capability, particularly in under-resourced jurisdictions. However, these recommendations reveal an implicit bias toward federal control over elections, as they propose placing agencies like **DHS** and **CISA** at the forefront of implementing and enforcing these standards. By doing so, the authors advocate for a system that diminishes state sovereignty and prioritizes centralized oversight—a sharp departure from the constitutional principle of state-led election administration.

The recommendations also highlight the importance of public-private partnerships in addressing election security challenges. Companies like **Microsoft, Amazon Web Services (AWS), Dominion Voting Systems**, and **CrowdStrike** are presented as critical allies in this effort, providing technological expertise and infrastructure to modernize

election systems. However, the authors fail to address the systemic risks associated with outsourcing critical election functions to private vendors. These companies often operate with little transparency and use proprietary systems that shield their processes from public scrutiny. This lack of accountability raises questions about the integrity of the systems they develop and their alignment with democratic principles.

One of the most striking omissions in this section is the absence of any meaningful discussion about compliance with existing federal laws and mandates, particularly **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF)**. The authors' failure to emphasize these requirements allows their recommendations to bypass the legal and ethical obligations that should underpin any effort to secure election infrastructure. Instead of reinforcing the need for rigorous compliance testing and third-party audits, the book advocates for the adoption of new systems and practices that often exacerbate existing vulnerabilities.

The authors also advocate for greater information sharing between federal, state, and local entities as a means of combating misinformation, disinformation, and cyber threats. While this proposal is framed as a collaborative effort to safeguard elections, it effectively institutionalizes the flow of sensitive voter data into centralized systems controlled by federal agencies and private vendors. The use of platforms like **Microsoft Azure** and **Amazon AWS** to store and analyze this data raises significant privacy concerns, particularly when these systems are subject to data-sharing agreements with agencies like **DHS** and **CISA**. By promoting these agreements without critically examining their implications, the authors contribute to the erosion of voter privacy and the centralization of election oversight.

Another key recommendation is the expansion of Risk-Limiting Audits (RLAs) as a standard practice for verifying election outcomes. While the authors present RLAs as a tool for enhancing transparency and public confidence, their implementation often necessitates the use of centralized data systems and detailed ballot manifests that compromise voter anonymity. The book fails to address the legal and ethical implications of these practices, particularly their violation of constitutional protections for anonymous voting and the risks they pose to voter privacy.

The book's overarching vision for election security reflects a troubling alignment with the interests of federal agencies and private vendors. By advocating for centralized standards, technological modernization, and expanded audits, the authors advance a

framework that consolidates control over election systems at the federal level. This approach not only undermines state sovereignty but also exposes elections to new vulnerabilities, including the potential for data breaches, cyberattacks, and systemic manipulation.

The book fails to reconcile its stated goals of transparency and accountability with the systemic risks introduced by its recommendations. The authors' reliance on centralized systems, private sector partnerships, and federal oversight creates a framework that prioritizes control over the fundamental principles of democratic governance. Their vision for election security, while ostensibly aimed at addressing vulnerabilities, raises significant concerns about its impact on voter privacy, constitutional protections, and the integrity of the electoral process.

"Securing the Vote" presents itself as a roadmap for protecting democracy but ultimately serves as a blueprint for centralizing control over elections. The authors' recommendations, while technically sophisticated, reveal a deeper agenda that prioritizes efficiency and oversight at the expense of transparency, accountability, and state autonomy. This final section, like the rest of the book, must be critically examined not as a solution to election vulnerabilities but as part of a broader effort to reshape the U.S. electoral system in ways that compromise its foundational principles.

The contributors and funders of ***"Securing the Vote: Protecting American Democracy"*** reveal the network of institutional, academic, and financial influence that has propelled the centralization of election systems under the pretense of modernization and security. This section demands critical examination as it establishes the foundation from which the book's proposals emerge, underscoring the coordinated efforts of federal agencies, private foundations, and prominent academic organizations to reshape the democratic process.

The primary contributors, listed under the auspices of the **Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology,** are aligned with prestigious entities such as the **National Academies of Sciences, Engineering, and Medicine (NASEM)**. The work was conducted through multiple specialized boards, including the **Committee on Science, Technology, and Law; the Policy and Global Affairs Division;** and the **Computer Science and Telecommunications Board.** This layered structure reflects the involvement of interdisciplinary expertise, ostensibly intended to ensure a comprehensive approach to election security. However, it also illustrates the

extensive reach of centralized academic and institutional players in framing policy and guiding public opinion on election reform.

The funding sources behind this publication are particularly illuminating. Grants from the **Carnegie Corporation** of New York and the **William and Flora Hewlett Foundation**, as well as support from the **W.K. Kellogg Foundation Fund** and the **Presidents' Circle Fund of the National Academies of Sciences, Engineering, and Medicine**, underscore the role of private philanthropic organizations in shaping the discourse on election security. These entities have a long history of influencing public policy through strategic funding, and their involvement raises critical questions about the agenda they promote.

The Carnegie Corporation, While its stated mission is to support the preservation and advancement of democratic values, its investment in ***"Securing the Vote"*** aligns with broader efforts to centralize election administration under the guise of combating misinformation and foreign interference. Similarly, the **Hewlett Foundation** has a track record of funding technology and governance projects that promote transparency and accountability, but its contributions to this project suggest a vested interest in advancing centralized data systems and audit methodologies like RLAs.

The Carnegie Corporation has been a significant funder of initiatives aimed at reshaping election systems and promoting democratic norms, both domestically and internationally. These efforts include support for the **National Voter Registration Act modernization projects, the Democracy Program at the Brennan Center for Justice,** and the **Partnership for American Democracy,** all of which aim to enhance voter access and reform election infrastructure. Internationally, the **Carnegie Corporation** has backed projects such as the **United Nations Development Programme (UNDP)'s Electoral Assistance Division,** which focuses on strengthening election systems in developing countries; the **International Institute for Democracy and Electoral Assistance (International IDEA),** which advocates for sustainable democracy worldwide; and collaborations with the **Carter Center** on election observation missions to ensure transparency and fairness in global elections. Additionally, it has contributed to initiatives like the **Open Government Partnership,** which seeks to improve government transparency and citizen participation on a global scale. These projects collectively reflect the corporation's commitment to embedding democratic norms, aligning election systems with global governance goals, and

promoting centralized oversight frameworks that integrate international standards into national practices.

The National Academies' Presidents' Circle Fund and the **Kellogg Foundation Fund** provide additional layers of influence. These funds are often discretionary and enable the **National Academies** to pursue projects that align with their institutional priorities. Their involvement in this project highlights the embeddedness of the academic establishment in driving policy recommendations that centralize election oversight. By framing these efforts as impartial and research-driven, these organizations obscure the political and systemic implications of their work.

The funding and support structure also reveals a deliberate effort to shield these proposals from scrutiny. The book explicitly states that the opinions, findings, and recommendations expressed do not necessarily reflect the views of the funding organizations. While this disclaimer is standard, it serves to distance the funders from accountability for the outcomes of the policies they promote. This distancing tactic creates an illusion of impartiality while allowing these organizations to advance their agendas under the guise of objective research.

The role of the **National Academies** in coordinating this effort is equally critical. As a respected institution with a long history of advising on public policy, its involvement lends credibility to the book's recommendations. However, this credibility must be interrogated in light of the systemic vulnerabilities and legal violations embedded in the proposals. By emphasizing the need for technological modernization, federal oversight, and public-private partnerships, the **National Academies** align themselves with an agenda that prioritizes efficiency and control over constitutional protections and voter sovereignty.

The funding and institutional backing of ***"Securing the Vote"*** also expose the broader context of election reform efforts in the United States. These initiatives are not isolated but part of a coordinated push by well-funded organizations and influential academic bodies to reshape election administration. The emphasis on RLAs, digital infrastructure, and centralized oversight reflects a convergence of interests among federal agencies, private vendors, and philanthropic foundations. This convergence raises serious questions about the motivations behind these efforts and the extent to which they serve the public interest versus the interests of centralized power structures.

The funding and institutional contributors to ***"Securing the Vote: Protecting American Democracy"*** reveal a network of influence that prioritizes centralized control over decentralized, state-led election administration. The involvement of organizations like the **Carnegie Corporation, Hewlett Foundation,** and **National Academies** highlights the ***role of private philanthropy and academic institutions in advancing an agenda that compromises voter privacy, state sovereignty, and constitutional protections.*** This foundation of influence must be critically examined as part of the broader effort to centralize election oversight under the guise of security and modernization. By framing their work as impartial and research-driven, these contributors obscure their complicity in undermining the democratic principles they claim to protect.

The publication of ***"Securing the Vote: Protecting American Democracy"*** in 2018, over a year after the issuance of **Executive Order 13800** and the establishment of the **NIST Cybersecurity Framework (CSF)** as binding federal law for critical infrastructure, underscores the deliberate omission of these legal requirements in the book's recommendations. Despite the authors' standing as leaders in academia and their significant funding from influential philanthropic organizations like the **Carnegie Corporation, the Hewlett Foundation**, and the **W.K. Kellogg Foundation**, their work conspicuously avoids addressing the mandates for compliance testing and third-party security audits required under federal law. This omission becomes even more significant when considering that the technologies and methodologies advocated in the book—such as centralized voter databases, Risk-Limiting Audits, and the adoption of proprietary systems—***are not only implemented in the United States but also exported globally through the same vendors and frameworks. The coordination between global philanthropic foundations and academic elites to promote these systems reflects a broader vision to centralize and standardize elections worldwide, eroding sovereignty and privacy under the guise of modernization and security. This timeline and its global implications expose a systemic agenda that prioritizes control over the democratic ideals it purports to protect.***

The document ***"Going from Bad to Worse"*** examines the vulnerabilities and risks inherent in modern election systems, with a focus on insecure voting technology and processes. Authored by prominent figures in computer science and election security, including **Dr. Ronald L. Rivest, renowned cryptographer and professor at MIT,** and other contributors closely associated with institutions like the **National Academy of Sciences,** this work seeks to expose the systemic flaws that have persisted in election

infrastructure despite decades of research and technological advancement. It critiques not only the state of current election systems but also the proposed strategies to address their weaknesses, framing these as necessary innovations to ensure election integrity. However, upon closer scrutiny, the document reveals a problematic reliance on centralized systems, federally coordinated frameworks, and private sector partnerships. ***This raises critical questions about the motivations of these academics, their funding sources, and the broader implications of the recommendations they advocate under the guise of improving election security.***

The central argument of ***"Going from Bad to Worse"*** is that without urgent action, election systems are poised to become even more vulnerable due to the continued reliance on outdated and insecure technologies. ***The authors detail how vulnerabilities in electronic voting machines, voter registration systems, and ballot tabulation processes have been exploited in past elections and could be exploited in future ones. They highlight specific weaknesses, such as the use of unauditable direct recording electronic (DRE) machines, insecure internet connectivity, and insufficiently protected voter registration databases.*** These critiques are valid and underscore the urgent need for reforms; however, the solutions proposed in the document reveal a reliance on centralized systems and private sector involvement that introduces new risks.

One of the most significant aspects of the document is its endorsement of paper-based voting systems and Risk-Limiting Audits (RLAs) as essential components of election security. While these measures are presented as solutions to the vulnerabilities inherent in electronic voting systems, ***their implementation necessitates the creation of detailed ballot manifests and centralized data storage. These systems require extensive metadata about ballots and voting processes, which, while crucial for statistical auditing, undermine voter anonymity and open the door to potential re-linking of ballots to voters. The authors fail to address these privacy concerns, instead framing RLAs as a panacea for election integrity.***

The document also critiques the fragmented nature of election administration in the United States, arguing that decentralization leads to inconsistent security practices and creates gaps that can be exploited by adversaries. While this critique is not unfounded, the proposed solution—a more standardized and federally coordinated approach—raises significant concerns. Centralized systems, by their very nature, create single points of failure that are more attractive targets for attackers. The document’s failure to critically

assess the trade-offs of centralization reflects a bias toward control and efficiency over resilience and privacy.

The funding and institutional context of the document must also be considered. The involvement of academic experts and their alignment with the same network of institutions and funders behind other election reform efforts, such as the Carnegie Corporation and Hewlett Foundation, suggests a coordinated agenda. The document does not operate in isolation but as part of a broader push to align election systems with centralized frameworks that are increasingly integrated with federal oversight and private sector technologies.

The technological recommendations in ***"Going from Bad to Worse"*** also highlight the reliance on private vendors like **Microsoft** and **Amazon Web Services (AWS)** for cloud-based storage and data processing. These partnerships are framed as necessary to modernize election infrastructure, yet they introduce dependencies on proprietary systems that limit transparency and accountability. The document's endorsement of these technologies without a critical examination of their risks reflects a broader trend in the election security discourse: prioritizing operational convenience and innovation at the expense of voter privacy and state sovereignty.

The timing of this document is critical. Published after the designation of elections as critical infrastructure under **DHS** in 2017 and the issuance of **EO 13800**, the authors ***were fully aware of the federal mandates requiring compliance with the NIST Cybersecurity Framework.*** Yet the document does not emphasize the necessity of adhering to these standards. Instead, it focuses on introducing new systems and methodologies that circumvent these legal requirements. This omission raises questions about whether the recommendations are genuinely aimed at enhancing security or facilitating the centralization of election oversight under federal and private control.

Furthermore, the document's critique of existing vulnerabilities does not adequately address the role of systemic neglect and noncompliance by election officials and private vendors. By focusing on the need for new technologies and frameworks, the authors divert attention from the accountability of those who have failed to secure election systems under existing laws and standards. This omission not only undermines the credibility of the document but also enables the continuation of practices that jeopardize election integrity.

In conclusion, ***"Going from Bad to Worse"*** provides a detailed and technically informed critique of the vulnerabilities in modern election systems, but its recommendations must be critically examined in the context of the broader agenda they serve. The document advocates for measures that centralize control, increase reliance on private vendors, and introduce new systemic risks under the guise of enhancing security. ***Its failure to emphasize compliance with existing federal cybersecurity standards and its lack of attention to the trade-offs of centralization reflect a deliberate alignment with the interests of federal agencies and private sector stakeholders***. This work, like others in the field, must be scrutinized not only for its technical merits but also for its role in advancing an agenda that prioritizes control over the foundational principles of democratic governance.

Securing the Vote RLAs.pdf - https://docdro.id/PAGNIZ9

going from bad to worse.pdf - https://docdro.id/dczm6lc



VIRGINIA VANDER ROEST

Training and Communications Manager, Michigan Bureau of Elections

Virginia Vander Roest is the Michigan Bureau of Elections Training and Communications Manager. 2019 is her 20th year working in election administration with the first 12 years being at the local level. Virginia is a CERA certified member of the Election Center, serving on past task forces and currently a member of the Investing in Elections Steering Committee.

Virginia Vander Roest represents a pivotal figure in the implementation and operational management of Risk-Limiting Audits (RLAs), deeply embedded within the ecosystem of **VotingWorks**, a private company based in San Francisco that developed the **ARLO** software. This system is essential to the administration of RLAs, as it determines which digital ballot images are selected for audits, a process that demands meticulous compliance with operational protocols. **Vander Roest's** role spans from her early career in **Michigan's** election systems to her **national influence in training election officials**, facilitating the adoption of **ARLO**, and ensuring rigorous adherence to its requirements.

Her career in election administration began in 1999 at the **City of Kalamazoo, Michigan**, where she served for 12 years. **Vander Roest** later advanced to the **Michigan**

Bureau of Elections, initially as an **Election Specialist focused on training local election administrators** and later as the **Training and Communications Manager**. In this capacity, she was instrumental in implementing **Michigan's** Risk-Limiting Audit project, reinforcing her role in shaping election practices tied to audit methodologies. This experience positioned her as a leader in operationalizing election security measures that align with centralized auditing frameworks.

Her expertise is further validated by her certification as a **Certified Elections/Registration Administrator (CERA)** through the **Election Center's Professional Education Program** in partnership with **Auburn University**. This program is the only continuing education initiative focused on voter registration and elections administration, underscoring her commitment to professional development. Beyond her technical certifications, **Vander Roest** has contributed significantly to the election community, serving on the steering committee for the **Investing in Elections research project** and **advising the Auburn University Graduate Certificate in Election Administration Board.** Her involvement with the **Election Center's Professional Education Program Certification Board,** which oversees the development of educational courses for election officials, highlights her influence in shaping election management standards across the nation.

In 2020, **Vander Roest** joined **VotingWorks** as the **Senior Election Implementation Manager.** In this role, she focused on scaling the company's capacity to support states conducting RLAs using its **open-source ARLO** software. Her transition to **VotingWorks** reflects a broader commitment to enhancing election security through the promotion and integration of centralized auditing technologies. As part of **VotingWorks**, **Vander Roest** has trained election officials across the country, ensuring strict compliance with **ARLO's** operational demands. This includes keeping ballots and metadata in order to align with digital ballot imprinting requirements, which, while technically necessary for RLA accuracy, create vulnerabilities that threaten voter anonymity and constitutional protections.

VotingWorks itself has played a central role in embedding RLAs into election systems nationwide. Contracts like the one signed by **Stuart Holmes,** the **unelected elections director** for the **Washington Secretary of State's Office**, highlight the expansive role the company plays. ***These contracts grant VotingWorks remote access to ARLO software during elections, with Holmes as the sole point of contact, bypassing oversight from Secretary of State Steve Hobbs.*** The lack of broader accountability

raises significant questions about the concentration of authority and the transparency of such agreements. Payments to **VotingWorks** reveal a broader scope of involvement in local elections than outlined in its contracts, with the company's role extending into direct election management, further blurring the lines between vendor responsibilities and election administration.

ARLO's functionality underscores the systemic centralization agenda facilitated by **VotingWorks** and **Vander Roest.** ***The software relies on detailed ballot manifests, precise metadata tracking, and centralized storage, ostensibly to improve audit transparency. However, these systems enable pathways for re-linking voter identities to ballots, undermining constitutional protections for voter privacy.*** **Vander Roest's** training and implementation efforts have ***directly contributed to embedding these processes into state election systems, aligning with federal oversight ambitions spearheaded by agencies like DHS and CISA.***

Documents and communications reveal **Vander Roest's** pivotal role in managing **ARLO's** integration into state systems. Her work ensures election teams adhere to **ARLO's** technical requirements while introducing significant reliance on digital tools and ***remote access***, inherently increasing cybersecurity risks. The broader implications of her work reflect a systemic push for centralized election oversight, consolidating control under the guise of transparency and security. These efforts align **VotingWorks** and **Vander Roest** with federal strategies to standardize election processes, often at the expense of state sovereignty and decentralized protections.

Virginia Vander Roest's influence extends far beyond operational management. Her previous roles with the **Michigan Bureau of Elections** and her leadership within professional election organizations reveal her deep integration into the national election infrastructure. By advancing centralized auditing practices through **VotingWorks** and the **ARLO** software, she has become a key player in transforming U.S. elections. However, the methodologies she promotes, particularly those ***reliant on metadata and ballot manifest tracking, raise significant questions about the erosion of voter privacy and state autonomy.*** Her contributions to embedding centralized control mechanisms into the electoral process demonstrate a broader alignment with federal and private sector agendas, raising critical concerns about the implications of her work for election transparency and integrity.

VotingWorks represents a critical player in the centralized election infrastructure landscape, with its open-source **Arlo** software serving as the backbone of Risk-Limiting Audits (RLAs) across the United States. The company markets itself as a solution for increasing election transparency and security, yet the documents provided paint a different picture, one of expanded control, potential vulnerabilities, and troubling operational practices. The company's reach extends beyond mere software provision; its involvement in pre-election setup, training, ballot handling, and election-day operations raises significant concerns about the boundaries between vendor responsibilities and election administration.

Central to **VotingWorks**' operations is the **Arlo** software, which determines which digital images of ballots are selected for audit during an RLA. The documents reveal that this software requires strict adherence to maintaining order among ballots, metadata, and manifests, creating a pathway for potential re-linking of ballots to voter identities. Despite claims of transparency, the technical requirements of **Arlo** demand centralized data management that inherently risks voter anonymity. ***The reliance on digital imprints and metadata for ballot auditing undermines constitutional protections for voter privacy.***

Beyond software, **VotingWorks** offers hardware solutions with capabilities that extend far beyond typical election administration needs. ***These systems are not only capable of scanning ballots but also printing them and altering choices on existing ballots.*** The implications of these functionalities are severe, as they ***introduce risks of election manipulation under the guise of operational efficiency.*** Documents detailing hardware specifications and configurations outline the seamless integration of these machines into **VotingWorks**' broader ecosystem, emphasizing their role in facilitating ballot processing and management.

The company's contract with **Washington State** further illustrates its expansive role in election administration. The agreement grants **VotingWorks** the ability to ***remotely access and service their software at any point during an election***. This level of access, combined with a **lack of oversight from the Secretary of State**, highlights a troubling consolidation of power in **unelected officials**, such as **Stuart Holmes. Holmes'** central role in the contract raises questions about accountability and transparency, particularly when critical election systems are effectively controlled by a private vendor.

VotingWorks' training programs also underscore its influence. By ensuring that election officials understand the operational intricacies of RLAs, **VotingWorks** embeds its methodologies into the core of election administration. However, these trainings often prioritize operational compliance over adherence to constitutional protections and federal standards. The documents reveal an emphasis on maintaining ballot order and metadata consistency, practices that, while technically necessary for **Arlo's** functionality, conflict with the principles of voter anonymity.

The hardware capabilities of **VotingWorks** further exacerbate concerns. Equipment designed to print ballots and alter choices introduces vulnerabilities that are antithetical to secure election practices. The capacity to combine paper and digital ballots seamlessly creates an additional layer of complexity, making it difficult to ensure that audits and recounts accurately reflect voter intent. Such functionalities, while marketed as innovative, open the door to potential abuses that undermine public confidence in elections.

The **ARLO** system represents the technological cornerstone of the Risk-Limiting Audit (RLA) process and serves as a crucial tool in what has been marketed as the advancement of election security and audit transparency. Developed and managed by **VotingWorks**, **ARLO** has been deployed across multiple states to operationalize RLAs, a statistical auditing method designed to verify election outcomes by comparing randomly selected paper ballots against the tabulated digital results. Despite its promises, **ARLO's** integration into election systems reveals complex layers of control, procedural precision, and potential vulnerabilities that demand scrutiny.

ARLO is a cloud-based, open-source platform that relies heavily on the input of precise ballot manifest data and sophisticated statistical algorithms to execute an RLA. The process begins with the creation of detailed ballot manifests, which are lists describing every batch of ballots cast in an election, often down to specific storage locations and physical ordering. This granular organization ensures that the system can track each ballot throughout the audit process, but it also introduces risks to voter anonymity. ***Maintaining the order of ballots, both physically and in metadata, inherently creates pathways for potential re-linking of voter identities to their respective ballots, contradicting the foundational principle of anonymous voting.***

Once ballot manifests are generated, the **ARLO** system employs a highly orchestrated method to select ballots for audit. This process is dependent on the generation of a

"seed" number, which is the input for **ARLO's** random number generator. This seed is determined through a public and ceremonial rolling of **ten-sided dice**, often performed in full view of election officials, observers, and sometimes the public. The seed is then entered into the **ARLO** system to generate the specific sequence of ballot batches and positions to be audited.

While this dice-rolling process is framed as a transparency mechanism, its reliance on precise human input and the subsequent digital computation raise questions about how randomness is ensured in practice. Once the seed is entered, **ARLO** calculates the audit trail, specifying which ballot batches and positions must be pulled for comparison against the tabulated results. **Election officials** are then tasked with retrieving these specific ballots and visually confirming their marks, comparing them to the corresponding digital records.

The **ARLO** system's statistical foundation lies in its ability to calculate a risk limit, the predetermined threshold for confidence that an election outcome is correct. The audit continues until the system verifies, within the specified risk limit, that the reported outcome is accurate or until a full hand recount is required. This statistical approach, while technically sound, is heavily dependent on the initial conditions of the system, including the quality of the ballot manifests, the accuracy of the seed entry, and the integrity of the random number generator.

Training election officials in the use of **ARLO** is an integral part of its implementation. Documents like ***"Knowing It's Right: A Practical Guide to Risk-Limiting Audits - Part One and Part Two and Three"*** reveal how officials are instructed on every aspect of the RLA process, from ballot manifest creation to the physical retrieval of ballots during the audit. The guides emphasize the importance of operational precision, requiring officials to adhere to strict protocols to maintain **ARLO's** functionality. For instance, officials must understand the statistical significance of risk limits and the procedural requirements for entering the dice-generated seed into the system. They are also trained to handle ballot retrieval in ways that minimize discrepancies, ensuring that the audited ballots align perfectly with **ARLO's** specified sequence.

Despite these trainings, the process introduces a high level of complexity, leaving room for errors, discrepancies, and vulnerabilities. The dependence on centralized cloud storage for **ARLO's** operations further compounds these concerns. ***Ballot manifests, audit data, and statistical calculations are often stored and processed in cloud***

environments, making them susceptible to breaches and unauthorized access. The involvement of **VotingWorks** as both the developer and **remote servicer** of **ARLO** exacerbates this vulnerability, as the company retains the ability to access and modify the system remotely under certain contracts, raising questions about oversight and accountability.

In addition to its technical operations, **ARLO's** adoption nationwide has been aggressively promoted by **VotingWorks**. The company positions itself as a non-profit, open-source alternative to proprietary election systems, emphasizing transparency and affordability. However, its deep integration into election processes, combined with its partnerships with state and local election offices, highlights its role in reshaping election administration. By providing not just the software but also the training, hardware, and ongoing support for RLAs, VotingWorks effectively embeds itself into the election ecosystem, exerting significant influence over how elections are conducted and audited.

The **ARLO** system, as implemented by **VotingWorks**, exemplifies the intersection of technology, procedural rigor, and systemic control in modern election audits. While it is presented as a tool for enhancing transparency and trust, its operational requirements, reliance on centralized data, and the potential for re-linking voter identities to ballots undermine these goals. The nationwide push for RLAs, driven in part by **VotingWorks**' advocacy and technical support, represents a broader trend toward centralizing election oversight under the guise of statistical validation and technological advancement.

The **ARLO** system operates as both a technical innovation and a mechanism for consolidating control over election processes. Its use raises critical questions about voter privacy, state sovereignty, and the role of private companies in public elections. The operational and procedural intricacies of **ARLO**, coupled with its broader adoption, highlight the need for a rigorous examination of its implications for democratic integrity. As **VotingWorks** continues to expand its footprint, the balance between technological efficiency and constitutional protections becomes increasingly precarious, demanding careful oversight and accountability.

VotingWorks stands as a case study in how privatization and centralization have quietly but profoundly reshaped the U.S. election landscape. While the company is often presented as a champion of transparency through its **open-source ARLO** software, its operational role in administering Risk-Limiting Audits (RLAs) exposes systemic vulnerabilities and raises critical questions about its outsized influence. Beyond its

technical offerings, **VotingWorks** has positioned itself as an indispensable player in implementing and managing RLAs nationwide, embedding itself deeply into both state and federal election infrastructures.

The company's involvement in training election officials, designing operational protocols, and maintaining direct access to election systems through **remote servicing agreements** highlights its sweeping control over processes that should remain independent. ***These roles go far beyond the scope of a typical vendor, allowing VotingWorks to dictate not just how audits are conducted but how entire election ecosystems are organized and monitored. This centralization, masked as efficiency, directly undermines the decentralization that has historically safeguarded the integrity and independence of state-run elections.***

Financial and contractual arrangements reveal further layers of concern. **VotingWorks**' agreements with states often grant it ***unchecked access to critical systems***, while payments and invoicing suggest a scope of involvement that exceeds public disclosure. These practices not only blur the lines between vendor and administrator but also ***eliminate essential safeguards against conflicts of interest and potential abuses of power.***

VotingWorks' alignment with federal priorities, particularly through its **partnership with DHS and CISA**, demonstrates its role in advancing a broader agenda of centralized election management. While ostensibly designed to enhance security, the company's systems rely on mechanisms that inherently compromise voter privacy and introduce avenues for potential manipulation. ***This alignment underscores how private companies, when left unchecked, can become instruments for advancing federal oversight at the expense of state sovereignty and public trust.***

In essence, **VotingWorks** is emblematic of the challenges posed by the increasing privatization of election infrastructure. Its influence over RLAs and election audits has introduced a concentration of control that is both unprecedented and unaccountable. By embedding itself into the core processes of election management, the company has altered the dynamics of electoral oversight in ways that risk undermining the foundational principles of transparency, voter anonymity, and decentralized control. The critical task moving forward is to expose and address these dynamics to ensure the integrity and independence of elections remain intact.

The document, ***"Ferry County Risk-Limiting Audit Pilot,"*** provides a detailed narrative of how the Risk-Limiting Audit (RLA) was conducted in **Ferry County Washington,** in April 2022. It highlights the operational procedures, technologies used, and outcomes of the pilot audit. The comprehensive analysis of the pilot reveals several key insights into how RLAs function, the pivotal role of **ARLO** software, and the importance of meticulous organization and chain-of-custody protocols to ensure audit accuracy. It also underscores how deeply embedded these systems are within election infrastructure, relying on strict physical and digital alignment of ballots and manifests.

The RLA in **Ferry County** was centered on a single contest—**School District 309 Proposition No. 1.** ***The process began with the preparation of a ballot manifest, which meticulously cataloged the ballots in storage by container, tabulator, batch ID, and ballot count.*** This manifest served as the roadmap for retrieving specific ballots during the audit. In parallel, the election system's **Cast Vote Record (CVR),** an electronic record of every scanned vote, was exported. Both the **manifest** and the **CVR** were uploaded into **ARLO**, **VotingWorks**' audit software, enabling the random selection of ballots for review.

The ballot retrieval process involved using a counting scale to identify the specific ballot selected by the ARLO software. By weighing ballots and programming the scale with the weight of a single ballot, election officials could quickly and precisely isolate the required ballot from its batch. This step highlights the significance of maintaining ballots in exact order and adhering to the ballot manifest, as even minor discrepancies would undermine the integrity of the audit process. Each retrieved ballot was replaced with a placeholder sheet to maintain the sequence for future audits or reviews.

The **ARLO** system played a central role in generating the random seed used to select ballots. This seed, derived through a public and participatory process of rolling ten-sided dice, ensures transparency and prevents any pre-determination of selected ballots. **ARLO's** pseudorandom number generator, powered by this seed, identified the specific ballots for audit, which were then retrieved and manually compared against the **CVR**.

Once retrieved, the audit board entered the voter choices for the sampled ballots into **ARLO** for comparison with the **CVR**. This step verified the accuracy of the voting system's tabulation, achieving a 97.4% confidence level in a single sampling round with no discrepancies detected. The audit report, including all technical specifications and the

list of audited ballots, was then submitted to the **Washington Secretary of State's office**, ensuring accountability and documentation.

The key takeaway from the **Ferry County** pilot is the critical role of strict ballot organization and chain-of-custody protocols. The use of the **ballot counting scale** significantly streamlined the process, reducing manual errors and increasing efficiency. However, this reliance on precise physical and digital alignment raises questions about vulnerabilities in larger-scale implementations, where the complexity and volume of ballots may increase risks of error or manipulation.

This pilot demonstrates the heavy dependence of RLAs on technologies like **ARLO** and the ***necessity for perfect coordination between physical and digital records.*** While the process in **Ferry County** was successful, the inherent reliance on centralized digital systems and the meticulous tracking of physical ballots highlight broader systemic vulnerabilities. ***These include potential risks to voter privacy, as ballot metadata and storage order can theoretically be used to trace ballots back to individual voters, undermining constitutional protections of anonymity.***

The document also reflects how RLAs and tools like **ARLO** are designed to centralize election processes under standardized frameworks, which may compromise the autonomy of local election officials. This centralization aligns with federal oversight strategies but raises concerns about the erosion of state sovereignty in election management. As **Ferry County's** pilot audit illustrates, RLAs require a balance between transparency, efficiency, and safeguarding voter rights—an equilibrium that current systems, including **ARLO**, struggle to achieve without introducing significant risks.

hannah_taylor@sos_wa_gov_06_01_2022_Ferry_County_RLA_pilot_full.pdf -

https://docdro.id/wvM4Prj

S-7150 Main Section.pdf - https://docdro.id/T26RJ2B

S-8028_VotingWorks Executed.pdf - https://docdro.id/Pz8z8RW

S-7150_VotingWorks_Executed Service_Contract_with_Exhibits_A-F.pdf -

https://docdro.id/S1ynyny

2019_DF_KnowingItsRight_Part1.pdf - https://docdro.id/9gan6Hr

Knowing Its Right Part 2 and 3 - https://docdro.id/5n6LNmH



SHANTIEL SOEDER

Election and Compliance Administrator, Cuyahoga County Board of Elections

Shantiel Soeder is the Election and Compliance Administrator of the Cuyahoga County Board of Elections and has been serving the voters of Northeast Ohio since 2005. During her tenure Ms. Soeder has played an integral role in ensuring accurate and transparent elections and led the initiative to become one of the first jurisdictions in the nation to implement risk-limiting audits in 2012.

Shantiel Soeder emerges as a prominent figure in the broader network of election administration, particularly through her role as the **Director of Election Services for Cuyahoga County, Ohio**. With her background in overseeing the operational and logistical elements of elections, her contributions intersect directly with pivotal aspects of election audits, cybersecurity, and the implementation of technologies such as Risk-Limiting Audits (RLAs). Her position places her at the nexus of state and county-level election management, bridging administrative processes with evolving federal oversight and private sector involvement.

This investigations documentation highlights her participation in various initiatives and committees that influence the direction of election processes nationally. For example, as a member of the **Bipartisan Policy Center's Elections Task Force**, she has contributed to discussions and frameworks aimed at modernizing election systems and improving audit practices. ***This task force, funded and supported by private philanthropic organizations like the Democracy Fund, functions as an influential advisory group, shaping policy recommendations that often align with centralized data-sharing practices and the adoption of Risk-Limiting Audits.*** **Soeder's** involvement suggests a clear alignment with the overarching agenda of embedding federally guided audit practices into state and county election systems.

In the the document detailing the **Bipartisan Policy Center's Elections Task Force Member Bios, Soeder** is described as a seasoned professional deeply involved in election security and auditing reforms. Her position in **Cuyahoga County,** one of the largest election jurisdictions in **Ohio**, gives her considerable influence over how these reforms are implemented. The county's use of RLAs and advanced audit technologies further underscores her operational role in ensuring compliance with both state and federally recommended practices.

From a broader perspective, **Soeder's** role is emblematic of the shift toward integrating county-level election management into federally influenced frameworks. Her responsibilities in **Cuyahoga County** include managing the logistical complexities of **ballot tracking, storage, and auditing,** all of which are crucial components of RLAs. ***The emphasis on precise ballot manifests and chain-of-custody protocols within her jurisdiction mirrors the methodologies promoted by VotingWorks and other entities central to the RLA infrastructure.***

Soeder's participation in national conversations on election security, combined with her operational expertise, positions her as a key implementer of audit technologies like **ARLO**. The document titled ***"BPC Elections Task Force Member Bios"*** reveals her active role in guiding discussions that support the adoption of RLA practices across diverse jurisdictions. However, this also raises questions about the degree to which county-level election officials, under the influence of such task forces, align their operational priorities with federally driven agendas.

The document also alludes to **Soeder's** role in providing training and guidance to other election officials, which aligns with the efforts of **VotingWorks** and federal agencies like **CISA** to standardize audit practices nationwide. ***This training often emphasizes maintaining the order and organization of ballots, ensuring that ballot manifests can be reconciled with digital records—a practice that, while operationally sound, creates vulnerabilities in voter anonymity and ballot traceability.***

The connection between **Soeder's** county-level responsibilities and her involvement in national task forces reflects the broader trend of using local election officials as conduits for implementing federally endorsed practices. This dynamic is particularly significant in the context of RLAs, where county-level compliance with audit methodologies directly feeds into centralized election oversight.

Shantiel Soeder's role highlights the intricate interplay between local election management and national audit initiatives. Her work in **Cuyahoga County** demonstrates the practical implementation of RLAs and advanced audit technologies, while her participation in national task forces underscores her influence in shaping broader election security policies. However, her alignment with federally guided practices raises critical questions about the balance between local autonomy and centralized control, particularly in the context of voter anonymity, data security, and the constitutional protections that underpin the U.S. electoral system. **Soeder's** contributions, while

operationally significant, must be critically examined within the broader investigative framework to understand their implications for election transparency, accountability, and sovereignty.

The Election Task Force, operating under the **Bipartisan Policy Center's (BPC)** broader strategy, is composed of a highly influential network of individuals spanning election officials, legal experts, academics, and private sector representatives. Named members include **Shantiel Soeder**, an experienced election official from **Ohio**; **Matt Masterson, former Senior Cybersecurity Advisor at DHS** and a prominent advocate for the federalization of election oversight; **Jennifer Morrell,** a consultant deeply embedded in Risk-Limiting Audit (RLA) implementation and training; **Stuart Holmes, Washington State's Elections Director** and **Treasurer of ERIC;** and **Virginia Vander Roest, Senior Implementation Manager at VotingWorks** and a key trainer in the use of **ARLO** software for RLAs. Additional individuals associated with the task force include **David Becker, founder of ERIC** and the **Center for Election Innovation and Research (CEIR); Tina Barton,** a former **Michigan** election official and proponent of centralized election oversight; and **Brenda Cabrera**, an election administrator heavily involved in task force-related training efforts.

The task force is closely connected to key federal agencies, including the **Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA)**, and the **Department of Justice (DOJ). DHS** and **CISA**, under the leadership of individuals like **Brandon Wales**, **Eric Goldstein**, and **Chris Krebs**, have played pivotal roles in embedding election infrastructure into the federal critical infrastructure framework. This collaboration with the task force has allowed these agencies to exercise considerable influence over state and local election practices.

The private sector is also well-represented in the task force's operations, with companies like **Microsoft, Amazon Web Services (AWS), CrowdStrike, Dominion Voting Systems, ES&S**, and **VotingWorks** providing the technological backbone for election systems. Individuals like **Tom Burt of Microsoft**, a leading voice in election security, and key representatives from **VotingWorks**, including **Ben Adida** and **Virginia Vander Roest**, actively contribute to the task force's initiatives. These entities develop and maintain the software and hardware critical to election systems, including tools like the **ARLO** software for RLAs, cloud storage solutions, and cybersecurity platforms.

Academics and researchers form another crucial pillar of the task force. Prominent contributors include **Dr. Philip B. Stark** of the **University of California, Berkeley,** who ***pioneered RLA methodologies***, and **Kellie Ottoboni**, a statistician who refined RLA statistical frameworks. Other contributors include **Dr. Ronald L. Rivest**, a computer scientist and co-author of foundational election security studies, and **Matt Bernhard,** a cybersecurity expert whose research has shaped the technical aspects of election audits.

Nonprofit organizations like the **Brennan Center for Justice**, represented by **Wendy Weiser** and **Lawrence Norden**, and the **Carter Center,** led by **Mary Beth Goodman,** also play significant roles. These groups provide research, advocacy, and on-the-ground support for election security initiatives, often aligning with the task force's broader objectives of standardizing and centralizing election practices.

The task force's integration with state-level operations is further solidified through its partnerships with members of the **National Association of State Election Directors (NASED)**. **Stuart Holmes** exemplifies this connection, utilizing his dual roles in **Washington State** and **ERIC** to align state-level activities with the task force's agenda. Other state election directors and officials participating in task force efforts include **Neal Kelley, former Registrar of Voters for Orange County, California,** and a prominent voice in election administration, and **Scott Borling of Michigan**, known for his operational expertise in RLA pilots.

The scope of the task force's work is expansive, encompassing federal agencies, state officials, private vendors, academics, and nonprofit organizations. This comprehensive and interconnected structure reveals a deliberate strategy to embed centralized control mechanisms into the U.S. electoral system, using the guise of enhancing security and transparency to consolidate influence. Each named individual and organization plays a distinct role in advancing this agenda, raising profound questions about the implications for state sovereignty, voter privacy, and the integrity of the electoral process itself.

The Election Task Forces, as revealed in the documents and supporting materials provided, operate as comprehensive mechanisms designed to centralize and streamline election oversight at federal, state, and local levels. ***These task forces are comprised of a diverse set of stakeholders, including state election directors, federal agency representatives, cybersecurity experts, private sector vendors, and non-governmental***

organizations. Their expansive structure and strategic partnerships illustrate their extensive influence on the election landscape across the United States.

The task forces are interconnected with agencies such as the **Cybersecurity and Infrastructure Security Agency (CISA),** the **Department of Homeland Security (DHS),** and the **Department of Justice (DOJ)**. **CISA** serves as the primary driver of election security initiatives, providing guidance, resources, and intelligence-sharing capabilities to state and local election officials. **DHS** complements these efforts through its designation of election systems as critical infrastructure, effectively embedding federal oversight into traditionally state-managed processes. The **DOJ** plays a pivotal role in legal enforcement and ensuring compliance with federal election laws.

The objectives of these task forces are multi-faceted, aiming to protect election systems from cybersecurity threats, enhance transparency and public confidence, and address potential misinformation or disinformation campaigns. However, their goals extend beyond immediate election security concerns, as they also work to align state and local election practices with federal standards and directives. This alignment is often facilitated through the integration of technologies, such as Risk-Limiting Audits (RLAs) and digital election management systems, which require extensive data collection and analysis.

"The Protect2020 Strategic Plan", a guiding framework for these efforts, emphasizes the importance of partnerships with private sector vendors, including CrowdStrike, Microsoft, Dominion Voting Systems, Amazon Web Services (AWS), VotingWorks, Clear Ballot, ES&S (Election Systems & Software), Hart InterCivic, Smartmatic, and Tenex Software Solutions. These collaborations are critical in providing the technological backbone for election security initiatives but also raise concerns about the privatization of election oversight. Vendors are often responsible for developing and maintaining the software, hardware, and cloud infrastructure used in election systems, creating potential conflicts of interest and vulnerabilities that could compromise election integrity.

By incorporating private sector software like ARLO, DHS, CISA, and state election officials have reinforced a dependency on external vendors such as Microsoft, CrowdStrike, Amazon Web Services (AWS), Dominion Voting Systems, Election Systems & Software (ES&S), Hart InterCivic, Tenex, Clear Ballot, Smartmatic, Scytl, and Pro V&V. These vendors provide critical infrastructure components, including

cloud storage, digital ballot tracking systems, cybersecurity tools, voting machine integration, and certification services. This deliberate integration establishes a centralized election framework, consolidating control under a network of private companies and federal oversight. By embedding these technologies across states, federal agencies and election officials have created a tightly interconnected ecosystem that shifts significant portions of election management into the hands of private entities, raising concerns about conflicts of interest, systemic vulnerabilities, and the erosion of state sovereignty over election processes.

Additionally, the task forces play a significant role in managing public narratives around election security. Through coordinated campaigns and partnerships with organizations like the **Bipartisan Policy Center (BPC),** they aim to counteract misinformation and disinformation, fostering public trust in the election process. However, these efforts often prioritize the dissemination of federally approved narratives, potentially sidelining legitimate concerns about election transparency and accountability.

The Election Task Forces exemplify a comprehensive and coordinated effort to reshape the election landscape in the United States. While their stated goals of enhancing security and transparency are laudable, their methods and partnerships reveal a deeper agenda of centralizing control and aligning state-managed elections with federal standards. The involvement of private vendors, the reliance on advanced technological tools, and the overarching influence of federal agencies underscore the complex and multifaceted nature of these task forces. Their activities warrant critical examination, particularly regarding their impact on voter privacy, state sovereignty, and the broader principles of democratic governance.



MAYURI SRIDHAR
Graduate Student, MIT

Mayuri Sridhar is a Master's student studying Artificial Intelligence at MIT. She completed her undergraduate degree at MIT, double majoring in computer science and mathematics. Her research, under Prof. Rivest's supervision, focuses on statistics and optimization applied to election audits.

Mayuri Sridhar, as evidenced by her contributions and detailed focus on election audits, emerges as a key academic and technical expert influencing the implementation and refinement of Risk-Limiting Audits (RLAs) across the United States. **Sridhar's**

academic background, likely in statistical methodologies or a related technical field, lends credence to her central role in the development of ballot selection and audit methodologies, particularly her work on innovative sampling techniques like the **"k-cut" method**. This method, detailed in her Master's thesis and subsequent collaboration with **Ronald Rivest**, introduces a statistically robust mechanism to ensure random and unbiased sampling of ballots, a cornerstone of RLA integrity.

Her prominence in the election audit field is further solidified through her involvement with collaborative research and publication efforts aimed at optimizing RLA procedures. These contributions highlight **Sridhar's** ability to merge theoretical statistical concepts with practical applications in election systems, reinforcing the operational integrity of RLAs. **Sridhar's** work on ballot polling methodologies, in particular, has been instrumental in addressing the challenges associated with manual ballot selection, improving efficiency while maintaining the rigorous statistical underpinnings required for effective audits.

The broader context of **Sridhar's** contributions aligns closely with federal election security initiatives, as evidenced by the documents emphasizing the integration of private sector tools like **ARLO** and software independence requirements outlined in ***"Voluntary Voting System Guidelines (VVSG) 2.0"*.** Her work appears to bridge gaps between academic theory and practical implementation, particularly in addressing logistical challenges such as ballot tracking, imprinting unique identifiers, and maintaining chain-of-custody protocols. These operational enhancements are critical in upholding the credibility and legal defensibility of RLAs, particularly in states adopting these methods under federal and state election guidelines.

However, while **Sridhar's** technical contributions are undeniable, their alignment with the broader federal agenda of centralizing election oversight raises questions about the implications for state sovereignty and voter anonymity. The reliance on statistically driven audit methodologies, while improving transparency, necessitates meticulous organization of ballots and voter data, potentially exposing vulnerabilities in privacy and security. Moreover, the integration of her methodologies within federal frameworks underscores the influence of centralized agencies like **DHS** and **CISA** in shaping state-level election practices, further blurring the lines of jurisdictional autonomy.

Her influence extends to her collaborations with federal and academic entities in crafting audit methodologies that not only meet but are shaped by evolving federal mandates.

These collaborations, while fostering innovation, also highlight the interplay between academic expertise and federal policymaking, raising questions about the independence of state election systems in an increasingly centralized framework.

Mayuri Sridhar's contributions to the field of election audits underscore the pivotal role of technical and academic expertise in shaping modern election practices. Her work exemplifies the fusion of statistical rigor and operational practicality, ensuring that RLAs remain a robust tool for verifying election outcomes. However, the broader implications of her methodologies, particularly in the context of federal oversight and centralized control, warrant careful consideration to safeguard the principles of voter privacy and state autonomy in the electoral process. This dual perspective reflects the complexity of integrating innovative practices into a system fraught with legal, ethical, and operational challenges.



PHILIP STARK

Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley

Philip B. Stark is Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley. He works on inference and uncertainty in physical, biological, and social sciences. He serves on the Board of Advisors of the U.S. Election Assistance Commission and on the Board of Directors of Verified Voting Foundation.

Philip Stark emerges as a central figure in the academic and operational realms of election auditing, particularly through his development of Risk-Limiting Audits (RLAs). **Stark's** work, which originates from his expertise in statistics and his role as a professor at the **University of California, Berkeley,** has profoundly influenced the evolution of election security practices across the United States. His theories and methodologies are not merely academic but have been operationalized into tools and frameworks adopted at both state and federal levels.

Stark's creation of RLAs has been widely touted as a statistically sound method for verifying election outcomes. His work provides the mathematical foundation for these audits, introducing concepts like the **SUITE (Stratified Union-Intersection Tests of Elections)** methodology. While RLAs are presented as neutral tools to enhance transparency, their implementation has been instrumental in driving centralized election

oversight. **Stark's** involvement in state pilot programs and his collaboration with election officials underscore his role in embedding RLAs into standard electoral practices, a development that raises questions about voter privacy and state autonomy.

The documents reviewed reveal **Stark's** significant role in the design and operational deployment of auditing tools like **VotingWorks' ARLO** software. **Stark's** statistical methodologies have shaped the requirements for RLAs, which depend heavily on detailed ballot manifests and precise digital tracking. This operational structure necessitates a degree of centralization, as physical and digital election materials must be meticulously organized and accessible for the audits to function effectively. **Stark's** influence extends beyond the technical aspects, as his work has been instrumental in convincing policymakers and election officials of the viability of RLAs, thereby securing their adoption at a broader scale.

Stark's affiliations with federal agencies such as the **Cybersecurity and Infrastructure Security Agency (CISA)** and his collaboration with private vendors like **VotingWorks** reflect his integration into the national election security framework. Documents indicate that **Stark** has provided guidance and tools that align closely with federal oversight goals. His participation in federally organized workshops and task forces highlights his role in bridging the academic, state, and federal dimensions of election auditing.

A closer examination of his work raises critical questions. While RLAs are framed as tools to verify election integrity, their reliance on centralized data systems and digital ballot tracking creates vulnerabilities that are not adequately addressed in **Stark's** frameworks. His statistical models assume an ideal operational environment, often overlooking the practical and cybersecurity risks introduced by the very systems that RLAs depend on. This gap between theory and practice points to a potential blind spot in **Stark's** approach, one that has significant implications for the privacy and security of election systems.

Stark's role is further complicated by his influence on state election officials and their adoption of RLAs. His involvement in training sessions and pilot programs demonstrates his direct impact on the operationalization of these audits. However, this influence also implicates him in the systemic issues that arise from RLAs, including the erosion of voter anonymity and the increased dependency on federal and private sector tools. **Stark's** academic credibility and authoritative position have played a key role in

normalizing these practices, effectively embedding centralized oversight into decentralized electoral systems.

The uploaded documents also reveal **Stark's** engagement with broader election security narratives. His contributions to reports and frameworks often emphasize the statistical robustness of RLAs while downplaying the broader systemic implications of their adoption. This selective framing raises questions about **Stark's** awareness of or willingness to address the full scope of risks associated with his methodologies. His collaboration with entities like **CISA** and private vendors suggests a strategic alignment with centralized election oversight, whether intentional or incidental.

Philip Stark's work represents a dual-edged influence on election security. While his statistical innovations have advanced the technical capability to verify election outcomes, the systemic risks introduced by these methodologies cannot be ignored. **Stark's** role in promoting RLAs, his collaboration with federal agencies and private vendors, and his influence on state election officials highlight his pivotal position in the evolving landscape of U.S. election systems. His contributions demand critical scrutiny, not only for their technical merit but also for their broader implications on voter privacy, state autonomy, and the centralization of election oversight.

Philip Stark's methodology, though acclaimed in academic and electoral circles, exhibits glaring blind spots that undermine its purported mathematical rigor and practicality. His approach, central to the Risk-Limiting Audit (RLA) framework, operates on the assumption that all ballots in a given sample are legitimate and accurately represent the votes cast. However, this assumption is foolhardy, as it completely neglects the possibility of fraudulent ballots being introduced into the system, particularly through mechanisms like those enabled by the **MOVE Act**. When ballots are returned via email, for instance, the potential for tampering between their digital return and subsequent physical printing is substantial. Manipulated ballots would seamlessly enter the system, appearing authentic to both digital and physical audits. Consequently, RLAs comparing digital images to physical ballots would fail to detect any tampering, rendering the entire process moot in identifying such fraud.

Moreover, the statistical foundation of RLAs, often heralded as their greatest strength, collapses under scrutiny when applied to real-world electoral complexities. For example, the **ARLO** software randomly selects a small sample of ballots for audit—say, 25 out of 1,000. While this sampling is statistically sound in theory, it does not account for the

reality that fraudulent ballots, by their nature, would be spread across the larger pool. Without verifying the remaining 975 ballots, there is no guarantee of their authenticity. The math becomes meaningless when it assumes the absence of systematic fraud, which it cannot statistically prove with such a small sample size. Worse still, the RLA framework tolerates a margin of error, allowing a limited number of fraudulent ballots to go undetected without triggering a full hand-count audit. This is not just statistically negligent; it's operationally asinine.

The application of RLAs in response to candidate-initiated recounts further exposes its inadequacies. In some documented cases, RLAs have completely ignored the specific races in question, instead auditing randomly selected ballots from unrelated contests. This has led to situations where not a single ballot from the candidate's requested recount was audited, yet the process was still declared fair and sufficient to certify the election results. Such practices not only undermine the credibility of the audit but also insult the intelligence of candidates and voters alike, reducing the audit process to a bureaucratic formality rather than a meaningful verification of election integrity.

Stark's theoretical frameworks fail to address these practical flaws, raising serious questions about the real-world applicability and reliability of RLAs. The blind reliance on statistical models and the dismissal of systemic vulnerabilities reveal a myopic approach that prioritizes theoretical elegance over genuine electoral security. **Stark's** methods, while academically celebrated, fall apart under the weight of real-world challenges, making them not just inadequate but actively harmful to the integrity of elections they claim to protect. His work, and the blind faith placed in it by election officials, demands rigorous scrutiny and accountability to prevent further erosion of public trust in electoral processes.



CHRIS SWOPE

City Clerk, City of Lansing, Michigan

Chris Swope has a long history of public service, having served as an Ingham County Commissioner and policy analyst for the Michigan Senate. He was elected Lansing City Clerk in November 2005 and is currently serving his fourth term. He is the former President of the Michigan Association of Municipal Clerks and also serves on the Legislative Committee and represents the association on the Council of Election Officials.

Chris Swope, the current **City Clerk of Lansing, Michigan**, holds a pivotal role in the administration of elections within his jurisdiction, and his inclusion in the **Microsoft Innovation Lab convening** underscores his broader influence in the election oversight landscape. Known for his active engagement in modernizing election processes, **Swope's** participation in forums like the convening aligns with his reputation as an advocate for the adoption of secure and efficient election technologies. However, a closer look reveals the inherent contradictions in his public positions on election transparency and the realities of centralized control mechanisms, such as Risk-Limiting Audits (RLAs), which he supports.

Swope's engagement with RLAs and his advocacy for their adoption reflect a trend among election officials to align with federal narratives that promote these audits as the gold standard for election integrity. **The Microsoft Innovation Lab convening,** where **Swope** was a participant, served as a platform for ***state and local election officials, private sector vendors, and federal agencies to strategize on the integration of RLAs and related technologies into state election systems.*** **Swope's** presence at this event signals his alignment with efforts to centralize election audit processes under the guise of improving transparency and public trust.

In **Michigan**, **Swope** has been an outspoken proponent of reforms aimed at increasing voter access and election security. While these efforts are publicly framed as measures to enhance voter confidence, they also align with the broader push for the adoption of systems like **ARLO** software, developed by **VotingWorks**. This software, integral to RLA implementation, has raised significant concerns about its implications for voter anonymity and the centralization of election data. As an election official endorsing these practices, **Swope's** role becomes central to understanding how these initiatives are operationalized at the local level.

Swope's involvement in the convening and his support for RLAs are particularly significant in the context of **Michigan's** evolving election infrastructure. The state's adoption of RLAs and related tools ties directly into federal initiatives led by agencies like **DHS** and **CISA**, which have advocated for centralized audit systems. As **City Clerk**, **Swope** is tasked with implementing these measures in a way that aligns with state and federal guidelines, a responsibility that places him at the intersection of local election management and national security frameworks.

Critically, **Swope's** participation in these initiatives raises questions about the balance between enhancing security and preserving the decentralized nature of U.S. elections. RLAs, while promoted as transparent and efficient, rely heavily on meticulous ballot tracking and digital data integration—processes that inherently risk breaching voter anonymity. The convening provided a forum for stakeholders like **Swope** to coordinate on these practices, highlighting his role in shaping local compliance with federally driven election security standards.

Furthermore, Swope's connections to vendors and other stakeholders involved in the convening reveal a broader network of influence that extends beyond Lansing. His position enables him to advocate for technologies and practices that, while framed as progressive, often align with the interests of private vendors and federal agencies rather than the decentralized electoral model traditionally upheld in the United States. This dual role as a local election official and a participant in nationally coordinated efforts places **Swope** in a position of considerable influence, but also exposes him to critiques of prioritizing federal directives over local autonomy.

Chris Swope represents a key figure in the operationalization of RLAs and the broader agenda to integrate centralized audit systems into state election processes. His advocacy for these measures, combined with his participation in platforms like the **Microsoft Innovation Lab convening**, underscores his alignment with federal and private sector initiatives aimed at modernizing elections. However, the implications of these efforts—particularly their impact on voter privacy, local autonomy, and the transparency of the auditing process—demand closer scrutiny. **Swope's** role exemplifies the challenges and contradictions inherent in balancing election modernization with the foundational principles of U.S. democracy.



MAURICE TURNER

Senior Technologist,
Center for Democracy & Technology

Maurice Turner is Senior Technologist at the Center for Democracy & Technology, where he focuses on the Election Security and Privacy Project identifying and updating election cybersecurity practices and infrastructure. He most recently served as a TechCongress Congressional Innovation Fellow assigned to the U.S. Senate Homeland Security and Governmental Affairs Committee, where he shaped policy and oversaw the preparation of memos, briefings, and hearings on federal IT systems and cybersecurity. He has also played an active role in local elections in CA and VA, holding progressively responsible positions from clerk to lead inspector overseeing multiple precincts. Turner holds an MA in Public Administration from USC, and a Certificate in Cybersecurity Strategy from Georgetown University.

Maurice Turner's involvement in election security, particularly his role in the **Microsoft Innovation Labs convening**, underscores his significant influence as a policy strategist and advocate for centralized election oversight. His work focuses on the intersection of technology, cybersecurity, and election integrity. **Turner's** leadership roles at organizations like the **Center for Democracy and Technology (CDT)** highlight his advocacy for implementing cybersecurity measures in elections while promoting transparency and voter confidence. However, his contributions also align with broader systemic shifts that raise concerns about voter privacy, state sovereignty, and the true independence of election systems.

Turner's role at **CDT** positioned him as a prominent voice in shaping narratives around combating disinformation, strengthening election security, and integrating technology into electoral processes. As a seasoned advocate for cybersecurity, Turner often frames his initiatives as essential for safeguarding democracy. However, his close collaboration with federal entities such as **DHS** and **CISA**, and private sector stakeholders like **Microsoft** and **CrowdStrike**, places him within the centralized framework that ties federal oversight directly to state and local election processes.

During the **Microsoft Innovation Labs convening, Turner's** input likely centered on aligning state election practices with federal guidelines, leveraging his expertise in technology policy. This convening was a pivotal event, bringing together figures deeply involved in the implementation of Risk-Limiting Audits (RLAs) and the broader

centralization of election oversight. **Turner’s** background in technology policy made him an essential contributor to discussions around integrating audit systems like **ARLO**, which depend heavily on centralized data collection and management.

Turner’s advocacy for voter confidence through enhanced cybersecurity measures must be critically examined within the broader context of his affiliations. His collaborations with private technology vendors that develop and maintain election systems reveal a potential conflict of interest. Companies like **Microsoft**, **Dominion**, and **VotingWorks** have benefited from such advocacy, which prioritizes federal and vendor-driven solutions over independent state election administration. **Turner's** promotion of these tools, while couched in the language of security and transparency, aligns with efforts to centralize voter data, potentially at the expense of privacy and state control.

In addition, **Turner’s** emphasis on combating disinformation intersects with narratives that dismiss legitimate public concerns as misinformation. This framing not only stifles critical discussions about election integrity but also reinforces the consolidation of authority among federal agencies and technology companies. His involvement in forums like the **Microsoft** convening reflects a strategy to institutionalize these narratives, embedding federal and private sector influence into election systems under the guise of countering threats to democracy.

Maurice Turner’s significant connections to cybersecurity policy extend beyond U.S. borders, aligning closely with global governance initiatives such as the **Open Government Partnership, the International Institute for Democracy and Electoral Assistance (International IDEA)**, and the **United Nations’ initiatives on election transparency and cybersecurity**. His advocacy frequently emphasizes the need for uniform standards and international cooperation in securing elections, which aligns with these organizations’ goals of embedding global frameworks into national policies. While this perspective seeks to address the challenges of an interconnected world, it also raises concerns about the erosion of national sovereignty. By integrating international standards into domestic election policies, **Turner’s** work reflects a broader agenda that prioritizes global uniformity, potentially at the expense of the unique legal and constitutional structures of individual nations.

Maurice Turner embodies the technocratic approach to election security that emphasizes centralized oversight, technological integration, and alignment with federal directives. His contributions to the convening and his broader advocacy work highlight a

commitment to embedding these systems into the electoral process. However, his role also raises critical questions about the implications of this centralization for voter privacy, state autonomy, and the independence of democratic systems. **Turner's** work illustrates the complexities and potential risks inherent in the intersection of technology policy, federal oversight, and election administration.

V1-RLA-Program-Final.pdf - https://docdro.id/kwGXmGC

The United Nations has positioned itself as a global leader in advancing election transparency and cybersecurity through a network of initiatives designed to enhance democratic practices worldwide. Key programs such as the **United Nations Development Programme (UNDP)'s Electoral Assistance Division** and the **Open Government Partnership (OGP)** exemplify the organization's commitment to fostering free and fair elections while promoting technological advancements in governance.

The UNDP's Electoral Assistance Division has supported more than 130 countries in strengthening electoral institutions and fostering transparent electoral processes. This initiative provides technical and advisory support to developing countries, including assistance in building robust voter registration systems, training election officials, and modernizing electoral technology. While these efforts aim to standardize and enhance election integrity, they also establish a framework for centralized election management that could undermine national autonomy.

The **UN's Open Government Partnership** focuses on promoting transparency and accountability by encouraging member states to adopt digital governance tools. This initiative extends into election security, emphasizing the importance of cybersecurity measures in protecting electoral systems from interference. However, the alignment of these initiatives with global cybersecurity frameworks, such as those promoted by the **United Nations Office of Counter-Terrorism,** demonstrates a trend toward integrating elections into broader international security strategies, which raises concerns about the potential erosion of national sovereignty.

Moreover, the **United Nations** has collaborated with organizations like the **International Institute for Democracy and Electoral Assistance (International IDEA)** and the **Carter Center** to promote best practices in election observation and monitoring. These collaborations often include the deployment of international election observers to ensure transparency and fairness. While these efforts contribute to credible

electoral outcomes, they also bring foreign oversight into domestic election processes, potentially infringing upon the principle of self-determination.

The **UN** has also emphasized the role of technology in securing elections, aligning with private sector leaders and global cybersecurity firms. Partnerships with entities like **Microsoft**, **CrowdStrike**, and **Amazon Web Services** are often brokered under the pretense of safeguarding electoral integrity. However, the reliance on these vendors introduces vulnerabilities related to data privacy, proprietary control, and potential conflicts of interest. These partnerships often promote centralized data systems, cloud-based storage, and digital ballot auditing tools that are increasingly adopted by member states.

United Nations' initiatives on cybersecurity further intersect with the recommendations of the **Global Forum on Cyber Expertise (GFCE)** and the **UN Office on Drugs and Crime (UNODC).** These bodies work to develop ***capacity-building frameworks*** for member states to combat cyber threats, including those targeting election systems. However, these frameworks often prioritize global standards over locally tailored solutions, potentially sidelining unique national and regional requirements.

The United Nations' overarching approach to election transparency and cybersecurity is rooted in a vision of global governance that seeks to harmonize democratic practices across nations. While this ambition is laudable in fostering cooperative efforts and setting high standards, it also introduces significant risks. The centralization of election management and cybersecurity strategies under international frameworks could diminish the capacity of individual nations to independently administer and secure their electoral systems.

The implications of this global agenda extend beyond technical support and standardization. By embedding international norms into election systems, the **UN's** initiatives risk creating dependencies on external actors, including private vendors and multinational organizations. This dynamic not only complicates accountability but also raises critical questions about the balance of power between national governments and international institutions in determining the future of democratic governance.

The adoption of Risk-Limiting Audits (RLAs) as a prominent election auditing method reflects the broader influence of international organizations and their partnerships with the **United Nations**. While the **United Nations** itself does not explicitly mandate RLAs, its advocacy for transparency, institutional capacity-building, and cybersecurity has laid

the groundwork for their integration into global election practices. International organizations like the **Carter Center** and **International IDEA**, both closely aligned with the **UN's** goals, have played significant roles in endorsing and facilitating the adoption of RLAs.

The Carter Center, a leader in election observation and democracy promotion, has advocated for rigorous audit mechanisms to ensure the integrity of election outcomes. It has specifically endorsed RLAs as a robust method for verifying election results, particularly in contexts where electronic voting systems are prevalent. By promoting RLAs in their mission to foster public confidence in election outcomes, the **Carter Center** has become a critical voice in standardizing such audits across democracies, including the **United States.**

International IDEA, an intergovernmental organization dedicated to advancing democracy worldwide, collaborates with the **UN** on initiatives aimed at improving election processes and safeguarding democratic governance. It has focused on providing technical assistance to countries exploring advanced audit methodologies, including RLAs. **International IDEA's** emphasis on evidence-based policy recommendations has contributed to RLAs being seen as a scientifically valid and transparent approach to election auditing.

The **UN's** broader agenda to modernize elections and enhance global trust in democratic institutions provides the necessary framework for these organizations to introduce RLAs as a solution. ***Its Electoral Assistance Division, under the UNDP, works in over 130 countries, promoting election standards that align with international best practices.*** While the division does not explicitly prescribe RLAs, its emphasis on rigorous auditing principles and transparency paves the way for their adoption, especially in nations seeking to align with globally recognized election frameworks.

Collaboration between the **UN**, the **Carter Center, International IDEA**, and additional entities such as the **Organization of American States (OAS)**, the **Electoral Assistance Division of the United Nations Development Programme (UNDP)**, and the **European Union Election Observation Missions** often leads to the propagation of shared methodologies and principles. This interconnected network of organizations facilitates the diffusion of RLAs without direct advocacy from the **UN** itself. By framing RLAs as an extension of broader goals like accountability, transparency, and public trust in

elections, these groups have indirectly contributed to their acceptance in multiple democracies.

The adoption of RLAs within this international context, however, raises critical questions about the broader implications of centralized election auditing methods. While framed as mechanisms to enhance transparency and trust, RLAs also introduce complexities tied to their reliance on detailed ballot manifests, statistical algorithms, and digital infrastructure. This reliance, combined with the influence of international organizations, highlights the global push toward standardizing election practices that may inadvertently compromise the autonomy of national election systems.

The endorsement and propagation of RLAs by organizations like the **Carter Center** and **International IDEA**, under the broader influence of the **UN's** transparency and trust-building initiatives, reflect a coordinated effort to standardize advanced auditing methodologies worldwide. While these efforts aim to strengthen electoral integrity, they also underscore the complexities and potential risks of aligning domestic election systems with globally driven frameworks.

Volume 4 of this investigation has laid bare a meticulously coordinated effort, spanning federal agencies, state officials, private vendors, and international entities, to centralize control over election systems while systematically undermining transparency, accountability, and the foundational principles of democratic governance. What has been revealed is not merely a failure of oversight or negligence but an orchestrated architecture designed to suppress independent scrutiny and mask vulnerabilities within critical election infrastructure. This systemic evasion of responsibility, reinforced by administrative policies, legislative measures, and international influences, has reshaped the electoral process into a mechanism of control rather than one of integrity.

At the heart of this volume lies the subversion of federal cybersecurity mandates, particularly **Executive Order 13800** and the **NIST Cybersecurity Framework (CSF).** These mandates, established to protect critical infrastructure—including elections—require independent third-party audits and rigorous compliance testing. Instead, state and federal actors, led by agencies such as **CISA (Cybersecurity and Infrastructure Security Agency)** and the **EAC (Election Assistance Commission),** have worked in tandem to circumvent these obligations. The substitution of genuine accountability with restrictive measures like Risk-Limiting Audits (RLAs) has further entrenched an illusion of security while perpetuating secrecy and obscuring systemic vulnerabilities.

The **Washington State** case study provides a chilling exemplar of this process. Under the leadership of figures like **Stuart Holmes** and **Bob Ferguson, Washington** implemented policies that directly contravene federal mandates, including amendments to **WAC 434-335-260** and the passage of **SB5459**. ***These measures eliminated third-party audits, denied public access to cast vote records (CVRs), and shielded election systems from independent scrutiny. Holmes' Clearinghouse Notice institutionalized these obstructions, codifying secrecy under the guise of security and further insulating the state's election infrastructure from lawful verification. This is not merely administrative oversight; it is a deliberate rejection of federal law and constitutional principles.***

Central to this investigation is the role of private vendors whose proprietary systems, third-party dependencies, and outdated software introduce critical vulnerabilities into election infrastructure. Vendors such as **Dominion Voting Systems, ES&S, Hart InterCivic, Smartmatic, Clear Ballot, Runbeck Election Services, BlueCrest, Scytl**, and **Unisyn Voting Solutions** have operated under a veil of secrecy, shielded by misapplications of the **Trade Secrets Act** and enabled by state contracts that permit self-assessments instead of mandatory compliance testing. **The SolarWinds Orion breach**, referenced throughout this investigation, highlights the catastrophic risks posed by these dependencies, which remain unresolved and unaccounted for due to the absence of independent oversight.

Compounding these issues is the entrenchment of advisory mechanisms over enforceable mandates. Entities like **CISA**, the **Center for Internet Security (CIS),** and **EI-ISAC** have positioned themselves as central coordinators of election security, yet their roles are advisory rather than regulatory. Their reliance on information sharing and voluntary participation has allowed systemic failures to persist unaddressed, as evidenced by the glaring omissions in exercises like ***Tabletop the Vote 2019*** and the ***Election Infrastructure Cyber Risk Summary***. The focus on reactive measures and narrative management, rather than prevention and compliance, reveals a fundamental misalignment with federal cybersecurity standards and an active resistance to transparency.

Furthermore, this volume exposes the global underpinnings of these policies. Risk-Limiting Audits (RLAs), championed domestically under the guise of enhancing election security, are now conclusively tied to international organizations such as **The Carter Center** and **International IDEA**, entities with close ties to the **United Nations.**

This connection is not coincidental but part of a broader strategy to integrate globalized election oversight mechanisms that prioritize centralized control over decentralized democratic processes. The implications of these ties extend beyond national governance, pointing toward an emerging framework of international influence that undermines **U.S.** sovereignty and public trust in elections.

The culmination of these findings reveals a stark truth: the current election security framework, as shaped by federal advisory agencies, state officials, private vendors, and international entities, is designed to protect itself rather than the democratic process it claims to serve. Transparency has been sacrificed for control, accountability has been replaced by secrecy, and compliance with federal law has been systematically obstructed. This architecture of control not only compromises the security and integrity of elections but also erodes the foundational principles of national sovereignty and self-governance.

As this volume concludes, it is clear that the domestic failures uncovered herein are part of a larger, more insidious agenda with global implications. The ties between RLAs and international organizations, such as **The Carter Center** and **International IDEA**, mark the beginning of a deeper investigation into the global forces shaping election systems. **Volume 5** will build upon these revelations, mapping out the network of ***dark money,*** global foundations, corporations, funds, and initiatives that have worked in concert to advance a new paradigm of governance—one that consolidates power under the guise of a so-called ***"new world order."*** By uncovering these connections, the next volume will expose how international influence, facilitated by ***dark money*** and aligned interests, is being leveraged to reshape democratic processes worldwide, subjecting not only the **United States** but also **130 other countries** to the same **international globalist control** driven by entities like the **United Nations, the World Economic Forum (WEF),** and **private foundations.** This scheme, under the guise of enhancing election integrity, poses ***a clear and present danger to human rights across the globe.*** By installing audit methods such as Risk-Limiting Audits (RLAs) that create a filing system capable of tracing votes back to individual signatures, these globalist forces are systematically dismantling voter anonymity and democratic principles. This represents not just a threat to **America** but a dire warning to all nations ensnared by this agenda—a coordinated effort to erode sovereignty and human freedoms in pursuit of a so-called ***"new world order."***