A Clear and Present Danger: How the Obama Administration Federalized Elections Through the Administrative State

Washington: A State Level Example

Attorney General Bob Ferguson, **Secretary of State** Steve Hobbs, **Elections Director** Stuart Holmes, **Governor** Jay Inslee, the **Department of Homeland Security (DHS)**, and **CrowdStrike** have, through gross negligence or intentional actions, failed to comply with critical federal mandates for cybersecurity and overstepped legal boundaries designed to protect state sovereignty in elections. Their collective actions undermine **Executive Order (EO) 13800**, and related **NIST cybersecurity frameworks**, creating vulnerabilities across Washington's election management and critical infrastructure systems.

Violation of Federal Cybersecurity Standards in Contract Requirements:

The contracts approved by **Attorney General** Bob Ferguson starting in January 2018—following the implementation of **EO 13800**—deviate from ***federally mandated cybersecurity frameworks*** **(NIST SP 800-53 and 800-171)**. Instead, Ferguson instituted a ***separate compliance "matrix,"*** which ***disregards federal law*** and ***replaces it with state-specific requirements, sidestepping federal cybersecurity mandates for critical infrastructure.***

- **Specific Omissions**: ***Federal cybersecurity standards would mandate third-party audits, extensive data protection protocols, audit trails, and independent compliance verification for systems as critical as election infrastructure. EO 13800's requirements for critical infrastructure specifically include these measures to protect against foreign and domestic threats.***
- **Intentional Bypass of Federal Law**: ***This replacement of NIST standards with a unique state framework indicates intentional actions to bypass EO 13800 and national security protocols meant to protect critical infrastructure from foreign and domestic threats.***

Systemic Failure in Independent Compliance Testing:

Rather than requiring independent, third-party cybersecurity audits mandated by **EO 13800**, the state has ***allowed contractors to self-assess compliance based on state-defined standards.*** This practice enables vendors to ***bypass rigorous federal compliance***, with Ferguson's framework institutionalizing a ***compliance workaround that effectively bypasses lawful third-party assessments.***

- **Impact of Self-Assessment**: Without independent audits, the accuracy of vendors' claims of compliance is **unverifiable**, relying solely on **self-assessment.** Federal standards require an **objective third party** to verify compliance to ***prevent unaccountable security lapses, which Ferguson's framework lacks.***
- **Systemic Non-Compliance and Accountability Failures**: Even if the contracts required adherence to **EO 13800**, every county would ultimately **fail key control groups**, including **Audit and Accountability** and **Information Integrity**, due to the state's refusal to release

cybersecurity data or Cast Vote Records (CVRs). Additionally, no ***third-party compliance assessments have been conducted or documented at the county level, violating federal expectations for critical infrastructure oversight.***

Proof of Non-Compliance Across All Counties:

Requests have been sent to every county in Washington for records proving federally required compliance testing conducted by independent third parties, with ***no county able to fulfill these requests.*** Responses from counties include:

- **Exemptions Claimed**: ***Several counties cited exemptions from releasing cybersecurity information and cast vote records, sidestepping EO 13800 mandates.***
- **Deflections**: ***Numerous counties claimed they were not required to follow EO 13800,*** directing inquiries to the Election Assistance Commission (EAC) or Federal Election Commission (FEC) or suggesting that questions be directed to the Secretary of State's office (OSOS).
- **Lack of Awareness**: Alarmingly, some counties were confused by the request, displaying a clear unfamiliarity with **EO 13800's** federal requirements for compliance testing and cybersecurity protocols for critical infrastructure.
- **Non-Response from OSOS**: A request was also sent to the OSOS for records of compliance testing since **EO 13800's** enactment on ***May 11, 2017***. ***No response*** has been issued, with counties and OSOS ***delaying any compliance record disclosure until after the election, in direct violation of federal law.***

These responses highlight that every county and the OSOS has been put on notice for failure to conduct federally required compliance testing since EO 13800 took effect, confirming a systemic non-compliance that has been perpetuated for years.

Inclusion of CrowdStrike's Role in Security Vulnerabilities:

CrowdStrike's Falcon platform recently experienced a ***significant breach in July 2024***, with a faulty update disrupting essential services in multiple sectors, including aviation and finance. This breach resulted in **widespread operational challenges**, prompting Delta Air Lines to file a $500 million lawsuit against **CrowdStrike** for gross negligence and operational losses. Despite **CrowdStrike's** transparency about its software dependencies, the platform's reliance on third-party libraries like **FastJSON and RapidJSON** has left it vulnerable to exploitation. This breach underscores **CrowdStrike's** vulnerabilities and ***its likely failure in compliance testing under federal standards such as EO 13800 and NIST requirements.***

- **Security Transparency with High Vulnerability**: Although **CrowdStrike** discloses its software dependencies, these dependencies, combined with third-party libraries, have ***proven highly susceptible to vulnerabilities, as demonstrated by recent security incidents in critical infrastructure sectors.***
- **Failure in Independent Compliance Testing**: Given **CrowdStrike's** reliance on these dependencies and the **recent breach**, the platform does not meet **EO 13800's** standards for critical infrastructure protection without extensive, federally compliant security redesigns and rigorous quality assurance.

Neglect Leading to National Security Threats:

The deviation from federal cybersecurity standards extends risks beyond elections, endangering critical infrastructure sectors that rely on the same systems. Previous cybersecurity breaches, like the **SolarWinds Orion hack** and **vulnerabilities exposed in CrowdStrike Falcon,** demonstrate the potential cascade effect of compromised systems on critical infrastructure:

- **SolarWinds Hack (2020)**: This breach, enabled by malicious code inserted into Orion software updates, impacted roughly 18,000 clients, including ***multiple U.S. government agencies. Hackers gained unauthorized access to sensitive systems across departments such as Homeland Security and Commerce. The breach's reach extended to critical infrastructure providers, raising concerns that access could be used to target systems essential for the power grid, water supply, and public safety networks.***
- **CrowdStrike Falcon Breach (2024)**: The recent breach in **CrowdStrike Falcon** due to a faulty update underscores the vulnerabilities embedded within **Falcon's** reliance on third-party libraries. This incident, which led to operational failures across aviation and finance sectors, illustrates the risks of an ***inadequately secured platform widely deployed across critical infrastructure sectors.***

This failure to adopt EO 13800 and NIST standards in election systems leaves the state vulnerable to similar threats, representing a significant risk to both state and national security.

Misuse of National Guard in Election Activities and State Sovereignty Infringement by DHS:

The **National Guard** has been deployed to assist with election-related tasks and public records requests, extending its role beyond traditional bounds. This deployment raises questions about the Guard's appropriate authority in state-managed election oversight and highlights potential misalignment with its designated, non-emergency functions.

National Guard's Involvement in Election Activities:

Utilizing the **National Guard** in election-related operations encroaches on the separation intended between civilian election management and military resources. This involvement stretches beyond typical Guard duties, prompting concerns about the balance between state election integrity and the presence of military resources.

State Sovereignty and **DHS** Engagement:

In addition to the Guard's deployment, the **Department of Homeland Security's** engagement in state election processes represents a ***significant overreach of federal authority***. Elections are traditionally within state jurisdiction, and ***federal involvement undermines state sovereignty***. Together, the **National Guard's** presence and **DHS's** role in state election functions create a complex issue, ***potentially infringing upon the state's right to independently and securely manage its elections.***

Unauthorized Amendments to Washington Administrative Code by Stuart Holmes and Randy Bolerjack:

Elections Director Stuart Holmes, an ***unelected public servant***, *further compromised election integrity by amending the Washington Administrative Code (WAC) using an emergency public*

health exemption. This amendment changed the classification of ***Cast Vote Records (CVRs)****, redefining them as ballots to restrict public access.*

- **Exploitation of Emergency Powers**: ***Holmes, in discussions with colleagues, drafted and implemented this emergency amendment, avoiding standard legislative review by using the public health exemption. This action prevented Cast Vote Records from being released and shielded election data from public scrutiny.***
- **Lack of Oversight and Bypassing of Elected Authority**: ***This amendment was not authorized by Secretary of State Steve Hobbs but was instead signed off by Deputy Secretary of State Randy Bolerjack, who has played a significant role in overseeing these changes. Bolerjack's involvement illustrates a troubling trend of authority delegation and a lack of oversight within the Secretary of State's office.***
- **Legislative Codification of Restrictions**: ***Once the legislature reconvened, SB5459 was passed, permanently banning the release of CVRs. The emergency amendments enabled this legislative shift, further consolidating restrictions on election data transparency under the guise of health and security.***

Failure of Oversight by Secretary of State Steve Hobbs and Elections Director Stuart Holmes:

Elections Director Stuart Holmes has also ***compromised the election system's security by signing contracts with VotingWorks***, allowing **remote access** to **ARLO** software used in ***risk-limiting audits, which opens a new vulnerability in election systems.***

- **Absence of Key Oversight by Hobbs**: **Secretary of State** Steve Hobbs, despite his role as the official overseer of elections, is **notably absent** in ***critical election documentation and decision-making***. Hobbs has delegated substantial responsibility to Stuart Holmes, who ***lacks both an electoral mandate and the necessary oversight bond.*** Hobbs's limited involvement and insufficient oversight of contracts, which originated from Ferguson's office, have allowed these ***systemic federal compliance violations to permeate Washington's election apparatus.***

Willful Neglect as Evidence of Intent and Potential Treason:

The disregard for **EO 13800**, failure to uphold **national cybersecurity standards**, and deployment of the National Guard in elections all signal **willful neglect** on the part of Ferguson, Inslee, Hobbs, Holmes, Bolerjack, and **CrowdStrike**. This **willful neglect** can suggest **intent**, especially given the heightened awareness of cybersecurity risks following the **2015 Office of Personnel Management (OPM) data breach** of 21.5 million federal employees.

- **Legal Grounds for Treason**: ***In matters of national security, willful neglect may be interpreted as intent, escalating these actions to potential treason. By disregarding federal law, sidestepping critical infrastructure protections, and leaving Washington's election systems open to domestic and foreign threats, these officials have collectively breached their oath to protect against "all enemies, foreign and domestic," creating severe risks for public safety, electoral integrity, and national security.***

Implications for Election Legitimacy and National Security

These compounded violations mean that no election in Washington State has been conducted lawfully or in compliance with federal cybersecurity mandates since EO 13800's issuance in 2017. The lack of adherence to national security standards and legal frameworks has led to a significant breach of federal law, fundamentally compromising the legitimacy of the state's elections.

In conclusion, the actions and decisions of Bob Ferguson, Jay Inslee, Steve Hobbs, Stuart Holmes, Randy Bolerjack, DHS, and CrowdStrike reveal a persistent failure to secure Washington's critical infrastructure, compromising election security and state sovereignty. Through intentional negligence or disregard for federal mandates, these officials and entities have allowed vulnerabilities that extend beyond state boundaries, exposing the nation's critical systems to potentially hostile actors. These breaches not only represent a profound violation of trust and duty but, given the scope and severity, could constitute acts of treason.

CISA's Role and Advisory Overreach

The **Cybersecurity and Infrastructure Security Agency (CISA)**, established in 2018 under the *Cybersecurity and Infrastructure Security Agency Act*, was designed as an advisory body within the **Department of Homeland Security (DHS)**. Its mandate focused on providing support and guidance to safeguard critical infrastructure across the United States, with a particular emphasis on cybersecurity. However, **CISA's** role has expanded considerably beyond its initial advisory scope, particularly in the area of election security. Although **CISA** lacks regulatory authority, it has exerted considerable influence over state election protocols, positioning itself as a central figure in election cybersecurity.

This expansion of influence has allowed **CISA** to guide states on election security measures, including practices that limit transparency around *public records, cast vote records (CVRs), and cybersecurity protocols*. These recommendations, framed as security measures, contradict the transparency and audit-ability requirements outlined in federal standards such as the NIST Cybersecurity Framework and Executive Order 13800, which mandate secure and transparent election processes.

When **Congress** established **CISA** in 2018, it was with a limited mandate to function as a supportive, advisory entity. The agency's intended role was to ***provide resources, expertise, and recommendations for protecting critical infrastructure sectors, including election systems, but without enforcement power.*** As an advisory body, **CISA** was positioned to collaborate with state and local governments, private entities, and federal partners in order to build resilience against cyber threats.

CISA's primary function was to share "best practices" and offer "voluntary tools and services" to help organizations enhance their cybersecurity posture. This role distinctly separated **CISA** from regulatory agencies like the **Department of Justice (DOJ)** and the **Department of Homeland Security (DHS)**, which hold direct enforcement authority. ***CISA's influence was meant to complement, not replace, regulatory oversight.***

Following the 2020 election and amid heightened concerns over election integrity, **CISA** expanded its focus on election security, issuing numerous advisories and resources targeted at state election

officials. Under the Biden administration, **CISA's** influence grew as it positioned itself as the go-to authority on election security matters. This shift effectively elevated **CISA** from ***an advisory capacity to a central figure influencing how states approached election security.***

Key examples of **CISA's** expanded role include:

Election Security Advisories: **CISA** issued guidance on election security protocols, frequently advising on practices that involved restricting access to public records under the premise of cybersecurity.

Guidance on Public Records and Cast Vote Records: **CISA's** advisories encouraged states to limit public access to sensitive records, including **CVRs**, to prevent potential security risks. However, this guidance often ran counter to **NIST's** transparency requirements.

Influence Beyond Advisory Capacity: Despite its ***non-regulatory status,*** **CISA's** recommendations were widely adopted by state officials, in part because of **CISA's** positioning within **DHS**, which ***lent its guidance a perceived authority that exceeded its advisory scope.***

A significant area where **CISA's** guidance diverges from federal standards is its ***advice on restricting access to election records, including CVRs and other public records.*** **CISA** framed this restriction as a necessary cybersecurity measure, ***advising that limiting public access would mitigate risks associated with data exposure***. ***This position has led to the passage of state laws restricting public access to election records, undermining transparency.***

CISA's recommendations on restricting CVRs ***conflict with the NIST Cybersecurity Framework,*** which prioritizes *transparency and audit-ability* in *critical infrastructure*.

By advocating for CVR restriction, **CISA**:

Contradicts **NIST's** *Audit and Accountability Requirements*: **NIST** mandates that systems handling critical infrastructure data, ***such as election systems***, maintain transparency to allow for ***independent verification.*** By restricting CVR access, **CISA's** guidance has ***undermined these requirements, limiting third-party auditing capabilities.***

Erodes Public Trust: The lack of transparency associated with restricted CVRs has fueled public distrust in election processes, as ***independent verification has been constrained by state policies influenced by CISA's guidance.***

CISA's role in election security has expanded beyond its initial advisory mandate, leading to a significant impact on state election policies and practices. Despite its lack of regulatory authority, **CISA's** guidance on restricting public records has had far-reaching consequences, influencing legislation that ***reduces transparency and conflicts with federal law***. This shift has left states in a precarious position, following guidance from an advisory body that has effectively ***sidestepped federal standards,*** undermining the *transparency and audit-ability* that the ***NIST Cybersecurity Framework and EO 13800 were designed to uphold.***

Federal Compliance Gaps

Executive Order 13800, signed on May 11, 2017, marked a pivotal point for securing U.S. critical infrastructure, including election systems. This order mandated that federal agencies adopt the

NIST Cybersecurity Framework to enhance *transparency, accountability, and resilience* in critical Infrastructure systems. For election security, **EO 13800** specifically required adherence to transparent auditing practices and third-party compliance assessments to ensure that elections remained secure and publicly verifiable. The **NIST Cybersecurity Framework**, a comprehensive and detailed set of cybersecurity standards, emphasizes essential principles such as *audit-ability, transparency, and third-party verification.*

However, despite these federal mandates, states have widely deviated from **EO 13800's** requirements. The root of this systemic non-compliance can be traced to advisory guidance from **CISA**, ***which has advocated practices that directly contradict NIST's transparency mandates, leaving states vulnerable to cyber threats and in violation of federal law.***

The **NIST Cybersecurity Framework** provides a structured approach to securing critical infrastructure and includes essential control groups, notably:

Audit and Accountability: This group mandates systems to maintain transparency and generate logs that allow retrospective analysis. For election systems, this includes *keeping cast vote records (CVRs) accessible for auditing to verify election results independently.*

Information Integrity: This group ensures data is complete, accurate, and secure. Transparency is crucial for election systems, where public trust relies on the ability to independently audit results and verify that votes are counted as cast.

Federal law, through **EO 13800**, requires that all election-related infrastructure ***comply with these NIST principles to secure U.S. elections against cyber threats.*** The intent behind these standards is to create an election system that is ***not only secure but also auditable, transparent, and accountable to the public.***

While the **NIST Framework** and **EO 13800** set clear expectations for *transparency*, **CISA's** ***advisory guidance has led states in the opposite direction***. **CISA's** recommendations have included ***guidance that actively restricts transparency around election data***, including:

Encouraging Restrictions on CVRs: **CISA** has issued advisories to states suggesting that ***access to CVRs could compromise election security***, framing these records as sensitive information that should be ***shielded from public access***. This guidance has ***influenced state legislation to restrict public access to CVRs, undermining NIST's audit-ability requirement.***

Misinformation on Public Record Security Risks: **CISA's** ***advisories have promoted the narrative that even harmless public records requests could pose security risks to election infrastructure. This guidance directly contradicts NIST's principle of transparency by suggesting that limiting access to these records enhances security, which federal law does not support.***

EO 13800 mandates the use of third-party assessors to conduct compliance testing for critical infrastructure systems, including election machines and software. ***Third-party assessments are intended to bring objectivity and expertise, as these assessors are trained to interpret and apply the NIST frameworks comprehensively, which is especially critical given the complexity of the SP800 series.*** By excluding independent third-party reviews, states risk inadequate cybersecurity compliance and unverified systems, opening pathways to systemic vulnerabilities.

However, **CISA's** recommendations to states have led to practices that ***sideline third-party compliance testing:***

Self-Assessment over Third-Party Verification: Under **CISA's** guidance, many states have adopted a self-assessment model for cybersecurity compliance, often approved by state **Attorney Generals.** This self-assessment approach diverges from **NIST's** requirements, as it lacks the objectivity and technical rigor that third-party assessments provide.

Undermining the Role of Third-Party Assessors: In high-profile cases like Colorado, election officials who attempted to secure independent assessments were met with severe legal repercussions. The case of **Tina Peters** exemplifies the risks that officials face when attempting to adhere to **NIST's** standards of transparency and independent oversight, demonstrating how deeply ingrained **CISA's *misleading guidance*** has become.

The widespread adoption of **CISA's** restrictive guidance has created a landscape where most states are ***out of compliance with the transparency and third-party assessment requirements set forth by EO 13800.***

This systemic issue is compounded by:

Lack of **DOJ** Oversight: Although the **DOJ** is the regulatory body tasked with ***enforcing compliance with federal laws, including EO 13800***, **CISA's *advisory status*** has allowed it to function as a shield. By positioning itself as the central authority on election security, **CISA** has effectively blocked **DOJ** intervention, leaving federal compliance **unenforced**.

Inadequate Accountability Mechanisms: Without enforcement from the **DOJ** or **DHS**, states have had free rein to adopt **CISA's** guidance, sidestepping **NIST** standards. The result is a lack of *accountability and transparency*, which is in ***direct violation of the cybersecurity expectations EO 13800 established for protecting critical infrastructure.***

Federal law mandates that all critical infrastructure, including election systems, adhere to the NIST Cybersecurity Framework's standards for transparency, audit-ability, and third-party verification. CISA's advisory guidance, however, has led states to implement practices that contravene these requirements, creating a widespread compliance gap that endangers the integrity of U.S. elections. By advising states to restrict public records and sideline third-party assessments, CISA has facilitated a departure from federal law, leaving election systems vulnerable and compromising the public's right to verify the security and accuracy of election outcomes.

Case Study – Tina Peters and Misuse of Advisory Influence

The case of **Tina Peters**, a former Colorado clerk who took actions to secure forensic copies of voting machines in Mesa County, Colorado, serves as a critical example of how **CISA's advisory influence has contributed to severe repercussions for election officials attempting to maintain transparency and compliance with federal records retention laws.** This case highlights the risks faced by election officials who, following their legal obligation to ensure transparency, encounter legal and institutional backlash. It also underscores the broader issue of how **CISA's *misleading guidance around election security and transparency has fostered an environment where actions aimed at complying with federal law can lead to punitive consequences.***

Tina Peters was responsible for overseeing Mesa County's election integrity, including ensuring the lawful retention of election records as required by federal law. Under federal regulations, election records, including digital records from voting machines, are mandated to be preserved for 22 months following a federal election. This mandate ensures that records are available for audits, transparency, and verification of election outcomes.

Ahead of a software update, referred to as a *"trusted build"* update, **Peters** took steps to secure forensic copies of Mesa County's voting machines. This action was taken to fulfill the federal requirement to retain election data, especially since such updates can potentially overwrite existing records, thereby violating federal retention mandates. **Dominion Voting Systems**, the voting machine vendor, assured officials that the trusted build would not delete any federally protected data. However, forensic analysis of the machines following the update confirmed that ***data had indeed been deleted, validating Peters' concerns.***

Peters' decision to create pre- and post-update forensic images aligned with her ***duty*** to protect election records for audit-ability. She sought assistance from a third-party assessor to analyze these forensic copies, ensuring impartiality and technical accuracy in verifying the election records. However, her actions led to ***criminal charges, including alleged violations unrelated to the forensic imaging itself, revealing the severe backlash faced by officials attempting to adhere to federal transparency laws.***

CISA's guidance, which has led states to restrict access to certain public records and downplay the importance of independent assessments, has had a significant influence on cases like **Tina Peters'**. Through its ***advisories***, **CISA** has promoted a model that ***frames transparency as a security risk***, ***advising states to restrict access to cast vote records (CVRs) and other election data, including machine records that are critical for public audit-ability.***

This ***advisory*** position has:

Influenced State Legislation: In Colorado and other states, **CISA's *advisories*** ***have encouraged legislation that restricts access to election records under the guise of security***. These laws have had direct impacts on how officials like **Peters** can handle election data, complicating efforts to *maintain transparency.*

Discouraged Independent Assessments: **CISA's** stance has effectively sidelined third-party assessors, who are critical to *upholding the transparency and accountability required* by the **NIST Cybersecurity Framework.** ***This contradicts federal law's intent, which prioritizes impartial compliance testing and audit-ability, especially in election security.***

The criminal charges brought against **Tina Peters** reflect how deeply **CISA's** guidance has ***misled state officials about election security compliance***. Rather than acknowledging **Peters'** actions as aligned with federal records retention law, Colorado authorities charged her with a range of offenses, effectively punishing her for attempting to uphold federal standards.

Key issues with the case include:

Failure to Recognize Federal Compliance Obligations: **Peters'** actions to secure election records were in line with federal law, yet the state prosecuted her as if her *transparency* efforts were a ***breach of security rather than an adherence to it.***

Exclusion of Critical Evidence: In court, **Peters** was reportedly barred from presenting evidence about her legal responsibility to retain election data or explain the necessity of her actions. Additionally, she could not reference her engagement of a third-party assessor, which ***federal cybersecurity frameworks demand as part of unbiased compliance testing.***

This case underscores how **CISA's** guidance, while ostensibly advisory, has shaped state responses to perceived "violations" of election security, leading to severe legal consequences for officials attempting to fulfill transparency obligations. By ***promoting a model*** that ***discourages independent assessments and emphasizes security over transparency***, **CISA's** influence has fostered an environment where officials like **Peters** face criminal prosecution for actions that ***align with federal law.***

The repercussions faced by **Peters** illustrate a broader issue of how **CISA's** guidance can create a culture of mistrust and punitive action toward election officials who seek transparency. This culture is particularly dangerous in an environment where officials are legally required to uphold federal standards, including transparency and public accountability.

The case of **Peters** exemplifies how, under **CISA's** influence:

Transparency Efforts Are Criminalized: Actions to secure forensic images and preserve records, which are ***mandated under federal law***, are treated as security risks, leading to criminal prosecution.

Federal Standards Are Undermined: **CISA's** guidance has led to practices that ***conflict*** with the **NIST Cybersecurity Framework's** requirements for *audit-ability*, effectively ***encouraging states to prioritize restrictive practices over legal transparency obligations.***

The case of Tina Peters is a clear example of the consequences that result when an advisory agency like CISA extends its influence beyond its intended scope. Through its misleading guidance, CISA has fostered a culture in which state officials are discouraged from transparency efforts, leading to punitive outcomes for those who attempt to comply with federal law. Peters' prosecution reveals the dangers of CISA's expanded role and underscores the urgent need for realigned guidance that prioritizes compliance with federal standards, transparency, and accountability.

Role of Federal Entities and State Attorneys General

The involvement of federal entities such as the **DOJ, FBI**, and state **Attorneys General (AGs)** is essential in ensuring compliance with cybersecurity mandates outlined in **Executive Order 13800** and the **NIST Cybersecurity Framework**. These agencies are responsible for overseeing and enforcing compliance across critical infrastructure sectors, including election security. However, **CISA's** influence has contributed to a deviation from federal standards, fostering a compliance model where states are allowed or even encouraged to sidestep mandatory federal guidelines. This installment explores how **CISA's** guidance, combined with the actions of state **Attorneys General**, has led to ***systemic non-compliance, undermining the security of the nation's critical infrastructure.***

The **DOJ** and **FBI** are the federal agencies primarily tasked with *enforcing federal laws*, including those related to election security and compliance with critical infrastructure standards.

Given the ***mandates*** established by **EO 13800**, these agencies should be actively involved in:

Ensuring Compliance with **NIST** Standards: **EO 13800** explicitly demands adherence to **NIST's** cybersecurity principles, particularly for *transparency, audit-ability, and independent assessments.*

Investigating Non-Compliance: As enforcement bodies, **DOJ** and **FBI** should address cases where states ***fail to comply with federal standards, particularly when it endangers national security.***

However, **CISA's advisory role** has created an environment in which the **DOJ** and **FBI** are effectively sidelined, with **CISA** positioned as the ***de facto authority on election cybersecurity.*** Since **CISA** ***lacks regulatory power***, its guidance ***does not carry the weight of law***; ***however, it has been perceived by states as official, allowing states to follow CISA's advice without DOJ intervention***.

This bypass has resulted in:

Lack of Investigative Oversight: Without **DOJ** and **FBI** investigations into state practices, non-compliance with **EO 13800** has gone unchecked, allowing states to ***deviate from NIST standards without repercussions.***
Reliance on **CISA's** Guidance Instead of Federal Law: **DOJ** and **FBI** have deferred to **CISA** on election security issues, treating its **advisory position** ***as if it held regulatory authority.*** This delegation of oversight to an **advisory agency** undermines **DOJ's** responsibility to enforce federal law.

State **Attorneys General (AGs)** hold significant influence over state election security practices, including the development and approval of compliance standards. Following **CISA's** guidance, many **AGs** have ***established compliance models that deviate from federal law by relying on self-assessment matrices, where election vendors are allowed to "self-certify" their cybersecurity measures.***

This practice:

Ignores Third-Party Verification Mandates: ***EO 13800 requires that election systems undergo independent third-party assessments to ensure impartiality and technical accuracy. Self-assessment matrices circumvent this requirement, allowing vendors to certify their own compliance without external verification.***

Creates Loopholes in Federal Compliance: By implementing self-assessment practices, **AGs** have allowed states to ***sidestep EO 13800's mandates.*** This approach has been approved by multiple **AGs**, enabling election vendors to ***bypass rigorous federal standards under state-implemented guidelines.***

CISA's influence has ***contributed to the development of these self-assessment matrices.*** By positioning its guidance as security-focused, **CISA** has allowed states to ***replace third-party assessments with self-certification models, creating an oversight loophole.*** This model, championed by **AGs** and state officials, has left election systems ***vulnerable to exploitation***, ***directly contradicting the NIST Framework's emphasis on independent assessments.***

The **Election Assistance Commission (EAC)**, like **CISA**, is ***an advisory agency*** that provides voluntary guidance and resources to support election security. Initially intended to assist with distributing federal grants for election improvements, the **EAC** began "certifying" election machines despite ***lacking regulatory authority.***

This shift has led to significant compliance issues:

Voluntary Guidelines Misinterpreted as Requirements: The **EAC's** guidelines were created as voluntary, but they are often interpreted by states as mandatory, similar to **CISA's** guidance. This misunderstanding has allowed vendors and states to ***rely on EAC "certifications" rather than adhering to NIST-mandated standards.***

Absence of Enforceable Standards: The **EAC's** guidance is non-binding, ***meaning that compliance with federal cybersecurity standards is effectively voluntary.*** This lack of enforceable standards has allowed states to ***circumvent federal law without consequence.***

Despite **EO 13800's** clear mandates, the **DOJ** has ***not pursued investigations or enforcement actions related to state election security practices that fail to meet NIST standards.*** This inaction can be attributed to the influence of **advisory bodies** like **CISA** and **EAC**, whose guidance has allowed states to ***operate under the perception of compliance without actually adhering to federal requirements.***

The **DOJ's** lack of intervention has:

Enabled Widespread Non-Compliance: By failing to investigate and enforce **EO 13800**, the **DOJ** has indirectly allowed states to follow **CISA** and **EAC's** ***advisory guidance as though it were legally binding.***

Undermined Federal Standards: The **DOJ's** deference to **CISA** and **EAC** guidance has ***weakened the enforcement of NIST standards, undermining the cybersecurity framework that is intended to protect the nation's critical infrastructure.***

The influence of **advisory agencies**, coupled with ***state-level self-assessment practices approved by AGs***, has led to a ***nationwide vulnerability in election security.*** Without **DOJ** and **FBI** enforcement, election systems are left vulnerable to cyber threats, particularly in the ***absence of independent third-party assessments***. ***The systemic non-compliance created by these practices has not only compromised election transparency but has also exposed other critical infrastructure sectors to potential exploitation.***

The **DOJ, FBI**, and state **Attorneys General** have a responsibility to uphold federal standards, particularly **EO 13800** and the **NIST Cybersecurity Framework**, to protect critical infrastructure. However, the advisory influence of **CISA** and **EAC**, coupled with *state-approved self-assessment matrices*, has created a system where ***compliance with federal law is bypassed under the guise of following "best practices."*** This lack of oversight has ***undermined the intended security of election systems, posing a clear and present danger to the nation's critical infrastructure.***

Nationwide Security Implications

The widespread deviation from federal standards for election security, driven by **CISA's advisory influence** and the lax enforcement of **EO 13800** by federal and state authorities, has ***created severe vulnerabilities not only in election systems but also across other critical infrastructure sectors.*** Examined herein are the broader implications of ***systemic non-compliance with federal cybersecurity mandates, revealing how weak election security standards can expose a range of critical infrastructure components—such as power grids, water systems, and the broader government network—to cyber threats. In essence, the issues with election security represent just the tip of a national security crisis that reaches into the core of America's infrastructure.***

The interconnected nature of the country's infrastructure means that a vulnerability in one system, particularly within election infrastructure, can open access pathways to others. This has been exemplified in cases like the *SolarWinds hack*, where ***a single vulnerability allowed attackers to infiltrate multiple agencies and private sector systems.***

The implications for election infrastructure, especially when lacking compliance with **NIST** standards, include:

Pathways for Lateral Movement: By exploiting election system vulnerabilities, attackers can use interconnected pathways to ***gain access to other systems within the same network, such as municipal or state-level infrastructure.***

Risks from Third-Party Dependencies: Many election systems depend on third-party software, such as ***CrowdStrike's Falcon platform***, which incorporates open-source dependencies like ***RapidJSON and FastJSON***—components historically exploited by state actors for cyber infiltration. ***Such dependencies create potential entry points for cyber actors to pivot from election systems to broader infrastructure.***

Federal law **mandates** that **all** *critical infrastructure, including election systems*, ***adhere to comprehensive cybersecurity standards as set forth by EO 13800 and the NIST Cybersecurity Framework***. This includes *ensuring transparency, third-party compliance testing, and the use of robust security protocols*.

However, **CISA's advisories** have led states to ***adopt fragmented cybersecurity measures, leaving election systems exposed to risks that compromise national security:***

Inadequate Transparency and Audit-ability: By discouraging the release of *cast vote records (CVRs)* and restricting public access to election data, states have compromised transparency, preventing independent verification and audit-ability. This lack of accountability also leaves critical vulnerabilities unchecked.

Absence of Independent Third-Party Assessments: **CISA's** guidance has led states to rely on ***self-assessment models approved by state AGs***, which are inherently less reliable than *independent assessments*. This approach ***directly conflicts with federal mandates requiring third-party evaluations to ensure objective and unbiased assessments of cybersecurity resilience.***

The vulnerabilities in election systems created by the ***lack of compliance with NIST standards*** extend far beyond election security. The interconnected nature of **U.S. infrastructure** means that a weakness in election cybersecurity can allow malicious actors to access other critical systems:

Energy and Power Grid Risks: Just as election systems depend on secure networks, the **U.S.** energy sector requires robust cybersecurity. Exploitable election system vulnerabilities ***could provide entry points into energy infrastructure, putting power grids at risk of being compromised.***

Water Treatment and Supply Facilities: Critical systems such as water treatment facilities often share cybersecurity resources with **municipal networks**, many of which include **election infrastructure**. An infiltration of election systems could allow attackers to ***pivot into water supply systems, disrupting essential services.***

National Defense and Security: The federal government relies on secure, interlinked systems for national defense, emergency response, and critical government functions. A breach in election infrastructure could ***expose entry points into broader government networks, leading to potential compromise of sensitive information and national defense protocols.***

Example: The **SolarWinds** Hack and Its National Security Implications

The **SolarWinds** cyberattack exemplifies the threat of interconnected vulnerabilities. In this incident, attackers leveraged a vulnerability in a widely used software update to ***gain access to multiple government agencies, infrastructure networks, and private sector companies.***

This hack exposed the inherent risks of fragmented cybersecurity measures across interconnected systems:

Chain Reaction of Vulnerabilities: The **SolarWinds** attack demonstrated how a breach in one sector can cascade into other areas of critical infrastructure. This same risk exists within election systems, where ***non-compliance with NIST standards*** creates exploitable gaps that can be used to ***access other critical networks.***
Undetected Exploitation of Dependencies: As seen in the **SolarWinds** case, attackers exploited ***third-party dependencies***, a tactic that remains **a significant risk** in election infrastructure due to the ***lack of rigorous third-party compliance testing mandated by federal law.***

The failure of election systems to comply with federal cybersecurity standards, compounded by **CISA's** restrictive guidance on *transparency and independent assessment*, has created a ***systemic weakness across the nation's critical infrastructure.***

The implications are severe:

Compromise of National Infrastructure: ***The systemic non-compliance introduced by fragmented election security measures exposes the U.S. to potential cyberattacks that could compromise essential infrastructure on a national scale.***

National Security Threats from Foreign State Actors: ***By weakening election infrastructure security, the U.S. has effectively left open pathways for foreign state actors, such as China, to infiltrate American networks. State actors could use these vulnerabilities to access sensitive data or disrupt infrastructure systems critical to national security.***

The nationwide non-compliance with federal standards for election security, driven by CISA's advisory guidance, has escalated from a cybersecurity oversight to a full-blown national security threat. The lack of transparency, independent assessments, and comprehensive cybersecurity measures not only jeopardizes the integrity of election systems but also exposes

broader critical infrastructure to cyber threats. This systemic issue, left unchecked, poses a clear and present danger to the safety and stability of the United States

The Urgent Threat of CISA's Planned Election Day Exercise

As Election Day approaches, **CISA** is planning a national cybersecurity tabletop exercise intended to test election security preparedness. However, given **CISA's advisory-only status** and the lack of regulatory authority, this exercise raises significant concerns regarding the ***agency's overreach and potential risks posed to election transparency.*** With **CISA** positioned as an **advisory agency,** there is ***no lawful basis for it to conduct an exercise of this magnitude on such a critical day***. This section underscores the urgent threat that **CISA's** planned exercise represents, especially in light of **CISA's advisory limitations**, and calls for the **Department of Homeland Security (DHS)** to take ***responsibility if this exercise proceeds under its jurisdiction.***

CISA, as an **advisory agency** within **DHS**, ***lacks regulatory or enforcement power over state election systems***. Its role has been to provide *guidance, resources, and cybersecurity support*; however, its **advisory scope** ***does not legally empower it to conduct or direct operations such as Election Day exercises.***

The planned tabletop exercise on Election Day not only steps beyond CISA's authority but also raises critical questions regarding:

Jurisdiction and Accountability: If **DHS** intends to proceed with this exercise, it should clearly state that it is doing so under **DHS's** direct regulatory authority. This *transparency* would place *accountability* on **DHS** to take *responsibility* for any consequences, miscommunications, or impacts of the exercise.
Potential to Obscure Real Threats: The exercise, scheduled on a high-stakes day, risks confusing the public, media, and officials. ***If a real cyberattack occurs during the exercise, it could be dismissed as a drill, allowing genuine threats to go undetected or under-reported.*** This lack of clear differentiation between exercise activities and real events could be exploited by malicious actors, ***further compromising election security.***

The planned exercise must be examined in the context of **CISA's** historical push to restrict *transparency* in election systems, particularly around *cast vote records (CVRs)* and other public records. Over time, **CISA** has advised states to implement restrictive security measures, influencing them to ***view transparency as a threat to security.*** This positioning contradicts ***federal mandates requiring audit-ability and transparency under the NIST Cybersecurity Framework.***

As **CISA** expands its influence, the exercise on Election Day appears to:

Further Obfuscate Public Access: With states already blocking access to key election records, an exercise conducted by **CISA** on Election Day itself could deepen these restrictions, ***creating confusion and potentially disrupting third-party assessments and public audits.***

Blur the Lines Between Advisory and Regulatory Power: By conducting an exercise on Election Day, **CISA** steps into an ***operational role typically reserved for regulatory agencies. This overreach implies regulatory authority that CISA does not possess, leading states to perceive its advisories as requirements and comply accordingly without legal basis.***

If **DHS** deems this exercise necessary, it should openly conduct it under **DHS** regulatory authority. By failing to clarify jurisdiction, **DHS** allows **CISA** to operate beyond its intended scope, with no accountability for the results of this exercise.

DHS's transparency is essential to:

Set a Clear Precedent for Accountability: An election security exercise conducted by **DHS** would require the agency to publicly account for any issues arising from the exercise, preventing **CISA** from ***operating in the shadows without liability.***

Ensure Public Trust: By declaring this exercise as an official **DHS** operation, the department would reassure the public that the exercise is ***supervised under appropriate authority, instead of CISA independently managing an exercise that could interfere with election day operations.***

An Election Day exercise of this nature presents an unusual opportunity for malicious actors, both domestic and foreign, to exploit the confusion surrounding a high-stakes cybersecurity drill.

This setup allows:

Malicious Exploitation of the Drill's Timing: Foreign adversaries or domestic cyber actors could capitalize on the exercise's timing, ***executing real attacks while the public and officials assume they are simulated incidents.*** This could lead to delayed responses and hinder incident detection and reporting.

Excuses for Obscuring Election Integrity Violations: If election irregularities occur, officials could cite the exercise as the cause, ***potentially disguising genuine issues as simulated events***. This ambiguity could ***undermine confidence in the election results***, particularly if incidents go unaddressed due to presumed drill activities.

To address these urgent concerns, the following actions are recommended:

DHS Should Assume Responsibility: If **DHS** deems the exercise critical, it should ***declare it a DHS-directed operation, not a CISA-managed event, with DHS assuming full regulatory responsibility for all aspects and outcomes.***

Immediate Public Disclosure of Exercise Intentions: **DHS** should disclose the full scope, purpose, and oversight mechanisms of the exercise to prevent any confusion or potential exploitation by malicious actors. Public awareness would allow citizens and officials to ***differentiate between drill activities and genuine threats.***

Delay or Postpone the Exercise: Election Day is ***not the time*** for ***experimental cybersecurity tests***. Postponing the exercise would allow the nation to focus on ***protecting election integrity without the distraction of a cybersecurity drill, thus reducing the risk of exploitation by adversaries.***

CISA's planned Election Day exercise exemplifies the risks of advisory agencies overstepping their authority, especially in high-stakes situations. Given CISA's non-regulatory role, this exercise threatens to create a shadow of confusion and ambiguity, potentially compromising the integrity of Election Day operations. The Department of Homeland Security should either take full responsibility for the exercise or delay it to avoid potential exploitation by malicious actors.

This issue underscores the urgent need to re-evaluate the boundaries of CISA's advisory role and prevent advisory influence from translating into unauthorized operational power.

The Department of Homeland Security (DHS) was established in the wake of the September 11, 2001, terrorist attacks, with the intent to unify and coordinate federal efforts to protect the United States from threats to national security. Several factors and legislative acts, particularly the USA PATRIOT Act, contributed significantly to the creation and expanded power of DHS. Here's a breakdown:

Creation of DHS and the Influence of the USA PATRIOT Act

1. **September 11, 2001, Terrorist Attacks**:
    - The 9/11 attacks exposed vulnerabilities in **U.S.** intelligence and security coordination, highlighting the need for a centralized agency to oversee homeland security efforts. In response, President George W. Bush proposed the formation of **DHS** as a means to consolidate and coordinate numerous federal agencies under one department.
    - **DHS** was officially established on **November 25, 2002**, through the **Homeland Security Act of 2002**, becoming one of the largest federal reorganizations in U.S. history. It unified 22 federal agencies, including the **Federal Emergency Management Agency (FEMA), U.S. Customs Service,** and the **U.S. Secret Service,** into a single department with a focus on homeland security.
2. **USA PATRIOT Act (October 2001) – "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"**:
    - Signed into law on **October 26, 2001**, the *USA PATRIOT Act* significantly expanded federal surveillance and investigative powers under the guise of combating terrorism.
    - The Act allowed for **enhanced surveillance** measures, including wiretaps, monitoring of email and internet communications, and access to financial, library, and medical records. It reduced restrictions on law enforcement agencies' ability to conduct searches and surveillance without traditional warrants.
    - Title II of the *PATRIOT Act* was particularly impactful, allowing for the use of **"sneak and peek" warrants** and expanded access to personal information through **National Security Letters (NSLs)**.
    - **FISA (Foreign Intelligence Surveillance Act) Court**: *The PATRIOT Ac*t gave new powers to the *FISA Court,* allowing law enforcement to obtain warrants without proving probable cause of a crime, focusing instead on national security and foreign intelligence. This led to an increase in **FISA violations** and surveillance abuses, as evidenced in multiple **DOJ** and **FBI** investigations in later years.
3. **Establishment of DHS as a Federal Surveillance Hub**:
    - The consolidation of agencies under **DHS** facilitated extensive domestic intelligence and surveillance operations. **DHS** established the **Office of Intelligence and Analysis (I&A)** to collect and analyze information about potential domestic threats.

- DHS also developed **Fusion Centers**, which work with local, state, and federal agencies to share intelligence on potential threats. These centers have been criticized for facilitating unwarranted surveillance of **U.S.** citizens, often without sufficient oversight or legal justification.
- Through Fusion Centers and inter-agency collaboration, **DHS** gained broad access to personal information under the guise of counter-terrorism, enabling domestic surveillance beyond foreign threats and including monitoring of activist groups, journalists, and ordinary citizens.

4. **Expansion of Surveillance and FISA Violations**:

    - Under the *PATRIOT Act's* provisions, agencies like the **FBI** and **NSA** have been able to conduct widespread domestic surveillance operations. Reports have documented **FISA violations** by these agencies, where surveillance tools meant for national security were misused for unauthorized monitoring of American citizens.
    - *FISA* applications often failed to disclose key details or contained inaccuracies, with a 2019 investigation by the **DOJ's** Inspector General revealing serious flaws in **FBI** *FISA* applications, particularly during investigations of **U.S.** citizens with tenuous foreign connections.
    - **DHS** also leverages **Section 702** of the *FISA Amendments Act,* which allows for the collection of foreign intelligence information from **U.S.** communications. While intended to target non-**U.S.** persons, **Section 702** has led to large-scale data collection on **U.S.** citizens, often incidentally capturing private communications without warrants.

5. **Rise of the DHS as a Centralized Federal Agency Control Mechanism**:

    - Since its creation, **DHS** has broadened its scope from counter-terrorism to include cybersecurity, disaster response, immigration enforcement, and even election security, especially since the Obama administration.
    - **DHS's** control over critical infrastructure sectors, enabled by **Executive Orders (EO) like 13636** and **Presidential Policy Directives (PPD) like PPD-21**, has expanded its jurisdiction over sectors previously under state control, including elections. This shift has centralized federal oversight across 16 critical infrastructure sectors, with **DHS** gaining increased authority to determine which sectors fall under its jurisdiction.
    - The 2017 designation of election systems as critical infrastructure extended **DHS's** control to state election systems, encroaching on state sovereignty in the management of elections. This shift has led to controversies over federal overreach and the loss of state autonomy, justified by national security concerns.

The establishment and expansion of **DHS** as a centralized control mechanism for national security issues has led to extensive surveillance practices, some of which exceed constitutional protections. Driven by the *USA PATRIOT Act* and a series of executive actions, **DHS's** mission has evolved from counter-terrorism to becoming a powerful agency with far-reaching oversight across sectors critical to both national security and daily life. ***This trajectory has fostered a culture of surveillance, eroding privacy rights, and, in some cases, violating FISA and civil liberties in the name of security.***

In particular, the PATRIOT Act's provisions, coupled with DHS's authority to classify state functions like election security as federal matters, have shifted significant power to the federal government, raising ongoing concerns about the balance between security and the preservation of individual rights and state sovereignty.

The Obama Administration's Slow Work Up to Federalizing Elections

The Obama administration laid the groundwork for **Secretary of Homeland Security** Jeh Johnson's 2017 designation of election infrastructure as critical infrastructure, partially through executive orders that broadened the **Department of Homeland Security's (DHS)** authority over cybersecurity and critical infrastructure.

Key executive orders that contributed to this shift included:

1. **Executive Order 13636 (February 2013) – "Improving Critical Infrastructure Cybersecurity"**:
    - This order directed the **DHS** to work closely with owners and operators of critical infrastructure to improve cybersecurity, particularly for sectors essential to national security and economic stability.
    - It laid out a framework for federal coordination with state, local, and private-sector entities, encouraging the creation of a ***cybersecurity framework (ultimately resulting in the NIST Cybersecurity Framework).***
    - This order gave **DHS** expanded authority to define and engage with critical infrastructure sectors, promoting a broader federal role in cybersecurity for national interests.
2. **Executive Order 13691 (February 2015) – "Promoting Private Sector Cybersecurity Information Sharing"**:
    - This order encouraged the private sector, as well as state and local governments, to ***share cybersecurity threat information with the DHS***, facilitating cross-sector collaboration on cyber defense.
    - It established **Information Sharing and Analysis Organizations (ISAOs),** which allowed **DHS** to ***coordinate directly with organizations and sectors, effectively expanding its influence and partnerships with entities responsible for critical infrastructure.***
3. **Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience (February 2013)**:
    - **PPD-21** redefined and restructured the nation's approach to critical infrastructure by emphasizing resilience and designating 16 critical infrastructure sectors.
    - It tasked **DHS** with taking a lead role in coordinating efforts to secure these critical infrastructure sectors and improving resilience across sectors that were deemed vital to national security and public safety.

- Although elections were not originally included as a designated critical infrastructure sector, this directive **empowered DHS** to designate ***additional sectors or subsectors as needed in response to emerging threats.***

Johnson's Justification and the Election Infrastructure Designation

These executive actions paved the way for Johnson to designate election systems as a critical infrastructure sub-sector under **DHS's** purview on **January 6, 2017**. ***He cited cybersecurity threats posed by foreign actors to the integrity of the electoral process as a national security concern***. By bringing election infrastructure under **DHS's** critical infrastructure framework, he aimed to ***provide states with access to federal resources and support for securing election systems, although this decision was controversial due to concerns about state sovereignty over election management.***

In summary, **EO 13636**, **EO 13691**, and **PPD-21** provided the basis for **DHS's** expanded authority in cybersecurity, enabling Johnson to justify the 2017 critical infrastructure designation for election systems by ***invoking the federal government's responsibility to protect critical infrastructure against cybersecurity threats.***

Executive Order 13800 (2017): "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Overview:

- Issued on **May 11, 2017**, this EO was aimed at enhancing the cybersecurity of federal networks and protecting critical infrastructure.
- It was a direct response to increasing concerns about **cyber threats** to national security, including threats to the **election systems** designated as critical infrastructure by DHS earlier that year.

Relevant Sections:

1. **Section 1: Cybersecurity of Federal Networks**:
    - This section mandates that all federal agencies manage their cybersecurity risks by adhering to the **NIST Cybersecurity Framework (CSF)**. Although it primarily focuses on federal networks, it sets the precedent for using **NIST standards** for managing risks, emphasizing that **NIST.SP.800-53** is the baseline standard.
    - The **NIST CSF** includes principles that originate from **NIST.SP.800-53**, especially regarding **risk management**, **control implementation**, and **security controls** for systems handling sensitive data. By referring to the **NIST CSF**, the EO indirectly makes the use of **NIST.SP.800-53** essential for managing election systems that have been categorized as critical infrastructure.
2. **Section 2: Critical Infrastructure Protection**:
    - This section specifically addresses **critical infrastructure sectors**, which, as of January 2017, include **election systems**. It directs the **Secretary of Homeland Security** to identify and prioritize efforts to mitigate the **risks** to critical infrastructure.

- For critical infrastructure sectors (like elections), the EO requires the implementation of **risk management** practices consistent with the **NIST standards** to secure these systems.
- The directive for **risk management** ties directly into the **NIST.SP.800-53** framework's emphasis on **assessing** and **managing risks** through a comprehensive set of security controls. Thus, to comply with the EO, election systems would need to follow the **NIST standards** before elections to ensure they are not vulnerable to threats.

3. **Section 3: Cybersecurity Reporting**:
    - It requires the **Heads of Federal Agencies** to submit risk management reports, including how they use the **NIST Cybersecurity Framework** to secure their operations.
    - While focused on federal agencies, this section underscores the necessity of **adopting NIST standards** as the primary mechanism for achieving **cybersecurity readiness**. Since the **election infrastructure** is part of critical infrastructure, state and local election systems are expected to follow these standards to ensure they meet **federal cybersecurity requirements** before an election.

How It Supports NIST Requirements for Elections:

- **EO 13800** sets a clear precedent that **NIST standards** are not optional but **required** for federal networks and critical infrastructure. By including election systems as critical infrastructure, it implies that states must adopt these standards to **secure election systems**.
- It enforces the **adoption of risk management practices** and **comprehensive testing** (as outlined in **NIST.SP.800-53** and **NIST.SP.800-171**) before elections to ensure **cybersecurity readiness** and **resilience**.
- The emphasis on **risk assessments**, **vulnerability management**, and **audit controls** directly aligns with the **Audit and Accountability (AU)** and **Risk Assessment (RA)** controls required in the **NIST** standards. Thus, state election systems must comply with these to meet the **federal mandate** for securing election infrastructure.

Executive Order 13848 (2018): "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election"

Overview:

- Issued on **September 12, 2018**, this EO focuses on addressing **foreign interference** in **U.S. elections**. It establishes the authority to impose **sanctions** on foreign entities and individuals involved in activities intended to influence or disrupt U.S. elections.
- It ties directly into the **cybersecurity of election infrastructure**, emphasizing the need for **election integrity**, **protection against cyber threats**, and **timely assessment of potential interference**.

Relevant Sections:

1. **Section 1: Assessment of Foreign Interference**:

- This section mandates that within **45 days** of an election, the **Director of National Intelligence (DNI)**, in consultation with relevant agencies, must conduct an assessment of any information indicating foreign interference in the election.
- The importance of conducting a timely assessment before and after elections aligns with the **NIST.SP.800-53** and **NIST.SP.800-171** focus on **continuous monitoring** and **incident response**. These frameworks require preemptive measures, testing, and readiness to ensure the system can detect and address any potential threats.

2. **Section 2: Reporting and Response**:
    - Requires that **agencies**, including the **Secretary of Homeland Security** and **Attorney General**, report on the impact of foreign interference on the security or integrity of election systems. This reporting process involves evaluating **cyber incidents**, which includes how vulnerabilities were managed and whether protective measures were in place before the election.
    - The **NIST.SP.800-53** framework emphasizes the need for **audit and accountability** and **reporting mechanisms** (AU control family). Election systems must demonstrate compliance with these standards by having **audit trails** and **log reviews** in place, making it easier to assess the impact of any interference.
3. **Section 3: Response Actions**:
    - This section details the types of **sanctions** and **measures** that can be imposed in response to interference, emphasizing the need for **clear standards** and **accountability** for those managing critical infrastructure like election systems.
    - The **focus on accountability** underscores the requirements set forth by the **Audit and Accountability (AU)** control in **NIST.SP.800-53**. It ensures that systems have the ability to **track and trace activities** to detect unauthorized access or tampering with the election process. This must be in place before elections to ensure readiness and compliance.
4. **Section 5: Sanctions and Enforcement Mechanisms**:
    - Specifies the **sanctions** to be imposed on foreign actors and entities involved in interference, but it also stresses the responsibility of **U.S. entities**—including those managing **election systems**—to ensure their infrastructure is not susceptible to foreign manipulation.
    - This section indirectly mandates that states adopt robust cybersecurity standards like those in **NIST.SP.800-53** to protect against potential foreign threats. The expectation is that **election systems must be tested and secured** against such threats before the election, reinforcing the importance of **pre-election compliance** with **NIST** standards.
5. **Section 6: Delegation of Authority**:
    - Grants the **Secretary of Homeland Security** and **Attorney General** the authority to take measures to address election-related cybersecurity threats.
    - This aligns with the **NIST frameworks**, as the **DHS** is already tasked with ensuring that critical infrastructure like election systems meets cybersecurity standards. Under

NIST.SP.800-53 guidelines, this includes conducting **security assessments** and ensuring **third-party evaluations** to validate the resilience of these systems.

How It Supports NIST Requirements for Elections:

- **EO 13848** reinforces the importance of **pre-election cybersecurity readiness**, ensuring that systems have been tested for **vulnerabilities** and **preparedness against foreign interference**.
- It supports the use of **NIST standards** by emphasizing the need for **audit trails**, **incident response mechanisms**, and **continuous monitoring**—all of which are critical elements of **NIST.SP.800-53** and **NIST.SP.800-171** frameworks.
- The requirement for **assessments** and **reporting** both before and after an election directly supports the **pre-election testing** and **validation** that **NIST** standards mandate to ensure that election systems are secure and **compliant with federal cybersecurity requirements**.
- The focus on **accountability** and **sanctions** reinforces that entities failing to meet these standards may face consequences, thus making adherence to **NIST cybersecurity protocols** effectively **mandatory** for states.

This breakdown of **EO 13848** highlights how it ties into the broader goal of securing election infrastructure, ensuring **NIST compliance** is part of the pre-election preparations. It emphasizes the critical nature of **security assessments** and the **reporting of vulnerabilities**, making adherence to **NIST standards** a central part of securing elections.

Executive Order 13771 (2017): "Reducing Regulation and Controlling Regulatory Costs"

Overview:

- Issued on **January 30, 2017**, this EO focuses on reducing the regulatory burden on federal agencies by controlling regulatory costs. It mandates that for every new regulation introduced, two existing regulations must be eliminated.
- While the EO primarily aims at reducing the volume of federal regulations, it has implications for the implementation and streamlining of **cybersecurity standards** like those of the **NIST.SP.800-53** and **NIST.SP.800-171** series by focusing on **efficiency** and **clarity** in regulatory requirements.

Relevant Sections:

1. **Section 1: Policy**:
    - This section establishes the policy that regulatory costs should be reduced, and for every new regulation introduced, at least two prior regulations must be eliminated.
    - For the **NIST standards**, this section emphasizes the need for **streamlined cybersecurity protocols** without adding additional regulatory burdens. It indirectly supports **NIST.SP.800-53** as a foundational standard that can be used as a **streamlined framework** for securing **critical infrastructure** like election systems.

- Instead of creating new and overlapping cybersecurity requirements, it ensures that **NIST standards** are adopted as the primary **regulatory framework** for critical infrastructure, ensuring clarity in expectations for states before they proceed with elections.

2. **Section 2: Cost Control**:
    - This section mandates that agencies, including those responsible for implementing **cybersecurity** and **critical infrastructure protection**, focus on reducing the cost of compliance by **minimizing duplicative regulations**.
    - This supports the role of **NIST.SP.800-53** and **NIST.SP.800-171** as **cost-efficient** frameworks for managing cybersecurity risks. Rather than creating new standards, agencies like **DHS** and the **Election Assistance Commission (EAC)** can rely on the **existing NIST frameworks** to meet federal requirements.
    - This approach ensures that **election systems** focus on **core cybersecurity controls** before elections, as defined in **NIST.SP.800-53**, without being burdened by redundant compliance measures.
3. **Section 3: Annual Regulatory Cost Submissions**:
    - Requires that agencies submit **annual plans** that include their regulatory actions and associated costs, which must reflect the principles of **regulatory reduction**.
    - This ties into the **NIST frameworks** because it means that **federal cybersecurity requirements**—like those set by **NIST** for critical infrastructure—are streamlined, clearly defined, and must be implemented without excessive additional costs. For **election systems**, this means relying on the **NIST standards** for **security testing** and **compliance checks** before an election as a cost-efficient solution.
4. **Section 4: Guidance**:
    - Directs the **Director of the Office of Management and Budget (OMB)** to provide further guidance on implementing the principles of **regulatory reduction**.
    - The **OMB's** role in coordinating with **NIST** to ensure that **federal cybersecurity frameworks** are applied efficiently without excessive regulations means that the **NIST standards** are maintained as a **core compliance framework**. This focus ensures that critical infrastructure, including **election systems**, must meet **NIST guidelines** in a streamlined manner before elections, ensuring **clarity and consistency**.

How It Supports NIST Requirements for Elections:

- **EO 13771** emphasizes the **streamlining** of regulatory frameworks, which indirectly **reinforces the central role of NIST.SP.800-53** and **NIST.SP.800-171** in securing election infrastructure.
- The focus on **efficiency** means that rather than creating new or complex cybersecurity rules, **existing NIST standards** are maintained as the **core set of requirements** for **pre-election testing** and **compliance**.
- By ensuring that compliance frameworks like **NIST.SP.800-53** are adopted without unnecessary layers of new regulations, the EO supports the notion that **election systems**

should focus on meeting **NIST cybersecurity standards** as the **primary method** for ensuring security before elections.
- This EO aligns with the goal of maintaining **consistent compliance requirements** for securing election infrastructure, making adherence to **NIST frameworks** more **cost-effective** and **centralized** for states, without undermining the robustness of the required **security assessments** and **controls**.

This analysis of **EO 13771** shows how it complements the **NIST frameworks** by emphasizing the need for streamlined and efficient regulatory compliance, allowing the **NIST standards** to remain as the primary guidelines for securing **election systems** before any federal election takes place.

Executive Order 13772 (2017): "Core Principles for Regulating the United States Financial System"

Overview:

- Issued on **February 3, 2017**, this EO establishes **core principles** for regulating the **United States financial system**, focusing on improving **economic growth**, **regulatory efficiency**, and **transparency**.
- While the EO primarily targets the financial sector, its emphasis on **transparency**, **accountability**, and **regulatory efficiency** directly relates to the implementation of cybersecurity standards like those of **NIST.SP.800-53** and **NIST.SP.800-171**. These principles are critical for ensuring that federal regulations, including those around critical infrastructure such as **election systems**, are applied consistently and transparently.

Relevant Sections:

1. **Section 1: Core Principles**:
    - The EO outlines **seven core principles** for regulating the financial system, several of which emphasize **accountability**, **regulatory efficiency**, and **fostering economic growth**. These principles include:
        - Empowering **American companies** to be competitive through consistent and clear regulatory frameworks.
        - Making regulation **efficient**, **effective**, and **appropriately tailored**.
        - Restoring **public accountability** within federal financial regulatory agencies.
    - While this section directly applies to the **financial sector**, it also sets a precedent for how **federal regulations** are to be implemented. In the context of **election systems**, it supports the idea that **NIST frameworks** (such as **NIST.SP.800-53**) should be applied in a manner that is **transparent**, **consistent**, and **accountable**.
    - For **election cybersecurity**, this means that **testing** and **compliance verification** must be conducted transparently before elections to ensure public trust in the process.
2. **Section 2: Coordination and Reporting**:

- This section directs the **Secretary of the Treasury** to consult with **members of the Financial Stability Oversight Council (FSOC)** and report on how well the existing regulations align with the **core principles** outlined in Section 1.
- In the broader context of **critical infrastructure regulation**—including **election systems**—this reporting mechanism reinforces the need for clear and **consistent regulatory practices**. It supports the requirement that **federal standards like those in NIST.SP.800-53** be used as a **benchmark** for evaluating and managing risks.
- The focus on **regulatory alignment** supports the expectation that **state election systems** should adhere to **national cybersecurity standards** like **NIST.SP.800-53** to maintain consistency and accountability, which is crucial for **election integrity**.

3. **Section 3: Review of Financial Regulation**:

    - This section requires a **review of regulations** to ensure that they meet the **core principles** and do not create unnecessary burdens. It encourages the removal or revision of regulations that do not add value or that hinder economic growth.
    - In relation to **NIST standards** for election security, this section underscores the importance of focusing on **effective, efficient, and targeted regulations**. The adoption of **NIST.SP.800-53** and **NIST.SP.800-171** as standardized frameworks for election systems ensures that states have a **clear set of controls** to follow, reducing **regulatory uncertainty**.
    - It ensures that **compliance checks** and **security assessments** are completed before an election to meet federal standards while avoiding unnecessary regulatory complexity. This is key to ensuring that **election infrastructure** is secure and compliant with **NIST frameworks**.

4. **Section 5: Accountability**:

    - Emphasizes the need for **transparency** in regulatory actions, requiring that regulatory changes and processes be **accountable** to the public.
    - This principle directly supports the **Audit and Accountability (AU)** control family within **NIST.SP.800-53**, which requires that systems handling sensitive information, like those in election systems, have mechanisms in place for **audit logging** and **review**.
    - By aligning federal regulations with principles of **transparency** and **accountability**, this section reinforces the need for **pre-election compliance assessments** to be conducted in a transparent manner, ensuring that election systems meet the **security controls** outlined in **NIST standards**.

How It Supports NIST Requirements for Elections:

- **EO 13772** emphasizes the importance of **transparent and consistent application** of federal regulations, which directly supports the need for **pre-election testing** and **validation** of election systems according to **NIST.SP.800-53**.
- The EO's focus on **regulatory efficiency** means that **NIST standards** are considered a **baseline for compliance**, avoiding the complexity of multiple overlapping regulations while ensuring that critical infrastructure is protected.

- It supports the requirement that **election systems** undergo **risk assessments**, **security testing**, and **audit processes** as outlined in **NIST frameworks** before elections to ensure **integrity and public trust**.
- By emphasizing **accountability**, the EO reinforces the need for **third-party verification** of compliance, making it clear that simply claiming adherence to **NIST** standards is not enough—there must be **verifiable evidence** of compliance before elections.

This detailed breakdown of **EO 13772** shows how it complements **NIST.SP.800-53** and **NIST.SP.800-171** by emphasizing **transparency**, **efficiency**, and **accountability** in regulatory practices, ensuring that election systems are held to a **consistent federal standard** before elections.

Executive Order 13891 (2019): "Promoting the Rule of Law Through Improved Agency Guidance Documents"

Overview:

- Issued on **October 9, 2019**, this EO focuses on **transparency** and **accountability** in the way federal agencies issue **guidance documents**. The goal is to ensure that **agency guidance** is clear, transparent, and does not create binding obligations beyond the authority granted by law.
- It requires agencies to make their **guidance documents** easily accessible to the public and ensures that such guidance does not serve as a **hidden regulation**. This EO is crucial in ensuring that agencies like **NIST** provide clear guidance on **cybersecurity frameworks** applicable to critical infrastructure, including election systems.

Relevant Sections:

1. **Section 1: Policy**:
    - This section establishes that **federal agencies** must **promote the rule of law** by ensuring that their guidance documents are transparent and publicly available. It emphasizes that guidance should **clarify existing regulations** rather than impose new, non-transparent obligations.
    - This aligns directly with the **NIST.SP.800-53** and **NIST.SP.800-171** frameworks, as it ensures that **NIST's cybersecurity guidance** for critical infrastructure is made clear and accessible to state and local entities responsible for **election systems**.
    - The EO ensures that **states** have **direct access** to the guidance required for implementing the **NIST cybersecurity standards** before elections, making it easier for them to understand and **comply** with the necessary security controls.
2. **Section 3: Public Access to Guidance Documents**:
    - Requires that each agency establish a **publicly accessible website** that contains all **guidance documents** in effect. It emphasizes that these documents should be presented in a way that is easy for the public and regulated entities to understand.
    - For **NIST frameworks** like **NIST.SP.800-53** and **NIST.SP.800-171**, this means that **cybersecurity guidelines** are required to be published and made accessible, ensuring

that **election system administrators** can **easily access the standards** they need to follow.
    - This transparency allows for **public oversight**, ensuring that the guidance on **security testing**, **audit controls**, and **compliance requirements** is not hidden from the public or those implementing these measures before elections.
3. **Section 4: Review of Existing Guidance Documents**:
    - Mandates that each agency review their **existing guidance documents** to ensure they are **consistent with law** and **properly issued**. Agencies must also ensure that their guidance does not impose obligations beyond what is legally required.
    - For **NIST standards**, this section reinforces that the guidance provided for **election security** must be clear and aligned with **federal requirements**, including those under **Executive Order 13800**. It ensures that the interpretation of **NIST cybersecurity controls** is consistent and legally sound, particularly in the context of **pre-election compliance**.
    - It means that **state election officials** must have access to **clear guidance** on implementing **NIST controls** like **Audit and Accountability (AU)**, **Risk Assessment (RA)**, and **System and Information Integrity (SI)**, ensuring that these controls are **properly implemented** before the elections.
4. **Section 6: Prohibition on Using Guidance Documents as Binding Law**:
    - This section clarifies that **guidance documents** cannot be used to impose binding requirements unless they are properly authorized by law. This ensures that regulated entities know what is required for **legal compliance**.
    - In the context of **NIST standards**, this means that while the **guidance** provided by NIST must be followed as part of federal mandates (as reinforced by **EO 13800**), states must clearly understand that **NIST standards are not optional** for securing critical infrastructure like election systems.
    - It ensures that states understand the **mandatory nature** of **NIST cybersecurity controls** as they relate to **pre-election security assessments**. This prevents any **misinterpretation** that might suggest that NIST standards are advisory rather than **essential for compliance**.
5. **Section 8: Implementation**:
    - Directs agencies to issue **guidance implementing this EO** within **120 days** and ensures that their compliance with **transparency** and **accessibility requirements** is maintained.
    - This section ensures that **NIST's guidance on cybersecurity standards**—including those in **NIST.SP.800-53** and **NIST.SP.800-171**—is accessible to all relevant stakeholders, ensuring that **election systems** have **clear directions** for how to achieve compliance before elections.

How It Supports NIST Requirements for Elections:

- **EO 13891** reinforces the **mandatory nature** of **NIST standards** by ensuring that **guidance** on these frameworks is accessible, clear, and transparent to all entities managing **election infrastructure**.
- The EO's focus on **transparency** ensures that state election officials and the public can **access** the necessary guidelines for **cybersecurity compliance**, making it clear what steps need to be taken **before elections** to secure systems.
- By requiring the **review and publication** of existing guidance, the EO ensures that **NIST frameworks** for **audit controls**, **risk management**, and **system integrity** are applied consistently and legally, emphasizing the importance of adhering to **NIST controls** as part of **pre-election security measures**.
- This EO supports **Executive Order 13800** by reinforcing that **NIST standards** are part of a broader framework for protecting **critical infrastructure**, and that compliance with these standards is necessary for **ensuring election integrity**.

This detailed analysis of **EO 13891** shows how it complements the implementation of **NIST.SP.800-53** and **NIST.SP.800-171** by emphasizing **transparency** and **clarity** in the application of these standards, making them a key component of **pre-election security** requirements.

Federal Information Security Modernization Act (FISMA)

The **Federal Information Security Modernization Act (FISMA)** is centered on the **cybersecurity** of federal information systems, including those systems related to election security. Its amendments in 2023, as outlined in the document you provided, place significant emphasis on:

- **Incident reporting** and **response plans** for cybersecurity threats.
- **Protection of critical infrastructure**, which includes election systems, from cyberattacks.
- **Vulnerability assessments** and the need for continuous **monitoring** to ensure system security.

However, there is **no mention** in the document that explicitly alters the requirement for **transparency** in election systems or negates the availability of **Cast Vote Records (CVRs)** for public audits.

Election Transparency and Cast Vote Records (CVRs):

FISMA remains consistent with previous legislative efforts to promote secure, auditable, and transparent systems, particularly those related to **critical infrastructure** such as elections. Under existing federal guidelines and frameworks (like **NIST.SP.800-53A**), transparency in election systems is maintained through:

- **Audit Trails**: Election systems are expected to produce **detailed logs** (including CVRs) that can be audited to ensure the accuracy and integrity of the voting process.
- **Public Accountability**: The release of **Cast Vote Records (CVRs)** ensures that the public, auditors, or third-party reviewers can verify that votes were accurately recorded and counted.

FISMA does not include provisions to eliminate this transparency. Instead, the Act is concerned with **security** measures to protect election systems from unauthorized access and tampering. In fact, a lack of transparency or failure to provide necessary audit records like CVRs could violate the principles of accountability mandated by federal cybersecurity frameworks, potentially opening officials to legal consequences.

Legal Grounds for Transparency and Audits:

- **Federal Compliance**: Election systems that interact with federal data or are secured under **FISMA** are still required to follow the **audit-ability and transparency requirements** found in the broader federal cybersecurity frameworks (such as **NIST**). Any failure to produce **CVRs** could be seen as non-compliance with these transparency and accountability mandates.
- **State Compliance**: In many states, transparency laws are in place that mandate the public release of **CVRs** or other audit mechanisms. Banning these records from public access could violate state-level transparency requirements and potentially lead to legal action or challenges based on public records laws.

Transparency vs. Security:

While **FISMA 2023** focuses on the **security** of election systems, it does not support the idea that security and transparency are mutually exclusive. Rather, the legislation reinforces the need to ensure election systems are both **secure** and **auditable** to maintain public trust. **FISMA** does not authorize election officials to hide or withhold **audit records** like CVRs in the name of security, and doing so would be against federal mandates for election integrity.

There is **no change in FISMA 2023** that removes the transparency requirements or legal obligations to produce **Cast Vote Records (CVRs)** for public audits. Blocking access to CVRs not only **erodes trust** in the election system but may also be a violation of both **federal transparency mandates** and **state-level public records laws**. These audit mechanisms are critical for ensuring the integrity and security of election results, and any attempt to ban them could be legally challenged as obstructing transparency in the democratic process.

The **National Cyber Strategy** and **President Trump's cybersecurity initiatives** emphasize a strong, cohesive approach to fortifying the nation's cybersecurity, which directly impacts the security of election systems.

The National Cyber Strategy

1. Defending the Homeland (National Cyber Strategy Pillar I)

The **National Cyber Strategy** places a critical focus on defending U.S. networks, systems, and critical infrastructure. Election systems, considered part of this critical infrastructure, are explicitly highlighted. The key elements include:

- **Securing Federal Networks and Information**: Election systems, such as voter registration databases and election management systems, often interact with broader federal networks. The strategy ensures centralized cybersecurity management through agencies like the

Department of Homeland Security (DHS) and **Cybersecurity and Infrastructure Security Agency (CISA)**. This centralized approach is crucial in applying consistent, high-standard security controls across all connected systems.

- **Improving Federal Supply Chain Risk Management**: With many election systems relying on third-party vendors, ensuring secure supply chains is vital. The strategy integrates supply chain risk management into procurement and risk assessment processes, ensuring that any technologies used in election systems are secure and resilient. By addressing vulnerabilities in the supply chain, the strategy works to prevent the introduction of risks into critical election infrastructure.
- **Securing Critical Infrastructure**: Election systems are part of the nation's critical infrastructure, and the strategy promotes a risk-based approach to cybersecurity. By prioritizing risk reduction in high-stakes sectors like elections, it aims to protect the systems from disruption by advanced cyber adversaries. This includes providing technical support and intelligence sharing to state and local election officials to prepare for and counter cyber threats.
- **Combatting Cybercrime and Improving Incident Reporting**: A critical part of election security is the ability to respond quickly to cyber incidents. The strategy encourages better incident reporting from all sectors, including election systems, to improve the nation's ability to detect and respond to potential attacks. This ensures that any threats to the integrity of election systems can be mitigated swiftly and effectively.

2. Promoting American Prosperity (National Cyber Strategy Pillar II)

A secure digital economy is key to national prosperity, and the **National Cyber Strategy** links this directly to cybersecurity in critical sectors, including elections. Some relevant actions include:

- **Incentivizing Cybersecurity Investments**: The strategy encourages private-sector partners and state governments to invest in strong cybersecurity measures for their systems, including election technology. It promotes better decision-making in cybersecurity investments by highlighting the importance of protecting sensitive data, including voter information.
- **Promoting Full-Lifecycle Cybersecurity**: Election systems are complex and involve many components, from voting machines to voter registration databases. The strategy encourages building cybersecurity into every phase of these systems, from design to deployment, ensuring that they remain secure against emerging threats throughout their lifecycle.

3. Preserving Peace Through Strength (National Cyber Strategy Pillar III)

A major goal of the **National Cyber Strategy** is to deter cyber adversaries from engaging in malicious activities. In the context of election systems, this pillar aims to prevent foreign and domestic actors from using cyberspace to disrupt democratic processes.

- **Deterring Malicious Cyber Actors**: By promoting strong cyber deterrence policies, the strategy helps protect election systems from being targeted by foreign adversaries seeking to interfere in U.S. elections. The establishment of consequences for malicious behavior in

cyberspace serves as a deterrent, reducing the likelihood of cyberattacks aimed at undermining election integrity.

- **Attributing and Punishing Cyber Attacks**: Ensuring that there are consequences for cyberattacks on critical systems, including elections, is a priority. By strengthening the government's ability to attribute and respond to attacks, the strategy makes it clear that any interference in the democratic process will face strong retaliation, potentially deterring future attempts.

4. Advancing American Influence (National Cyber Strategy Pillar IV)

Protecting the global internet infrastructure supports not only economic interests but also the integrity of democratic processes worldwide, including U.S. elections. The strategy promotes a secure and open internet, which is crucial for ensuring the transparency and integrity of the electoral process.

- **Promoting Secure Communications Infrastructure**: The strategy encourages secure and interoperable communications infrastructure, which is essential for supporting secure election processes. This includes protecting internet-connected systems that manage voter data and election results from tampering or disruption.
- **Building International Cyber Capacity**: By working with allies to strengthen their cybersecurity, the U.S. also helps create a more secure global cyber environment. This reduces the risk of foreign interference in U.S. elections and helps establish global norms of responsible behavior in cyberspace, further protecting democratic processes.

How These Strategies Bolster Election Security:

- **Holistic Protection**: The National Cyber Strategy’s comprehensive approach strengthens the overall security of election systems by addressing both technical and policy-based solutions.
- **Public-Private Partnerships**: The strategy emphasizes cooperation between government agencies, private sector partners, and state/local officials to secure elections, providing technical assistance, intelligence sharing, and best practices for election security.
- **Cyber Deterrence**: Deterring malicious actors, both foreign and domestic, from interfering with U.S. elections is a key priority of the strategy. By establishing clear consequences and strengthening cybersecurity measures, it creates a strong defense against election-related cyber threats.

In summary, the **National Cyber Strategy** provides a robust framework for securing election systems by integrating these systems into broader national cybersecurity efforts, promoting risk-based protection, and deterring malicious cyber activities that threaten the integrity of U.S. democratic processes. This multi-faceted approach helps ensure that election systems are resilient and capable of withstanding modern cyber threats.

National Cyber Strategy and Election Security

The **National Cyber Strategy**, along with policies from the **Trump administration**, established a robust framework for defending critical infrastructure, including election systems. Both strategies

focused on securing the digital landscape against foreign and domestic cyber threats, aiming to protect key democratic processes like elections.

1. Centralized Cybersecurity Management

The **National Cyber Strategy** emphasizes strengthening the **security of federal networks**, which includes election systems that interact with federal databases and rely on secure communication across state and federal platforms. This ensures that election-related infrastructure is protected by centralized cybersecurity standards, enforced by federal agencies like the **Department of Homeland Security (DHS)** and **Cybersecurity and Infrastructure Security Agency (CISA)**. These bodies provide state and local officials with resources, guidance, and real-time threat intelligence to safeguard election systems.

2. Securing the Election Supply Chain

Election systems, particularly those managed through third-party vendors, face potential supply chain vulnerabilities. The strategy tackles these risks by integrating **supply chain risk management** into cybersecurity practices, ensuring that hardware, software, and services used in election systems meet stringent security requirements. This approach helps prevent unauthorized access, malware infiltration, and tampering with critical election technology.

3. Continuous Monitoring and Threat Detection

A cornerstone of both strategies is the emphasis on **continuous monitoring** of critical infrastructure, including elections. Real-time detection tools and monitoring capabilities ensure that any irregularities or attempts at cyber interference are flagged and addressed promptly. The **NIST.SP.800-53** framework, which is closely aligned with the goals of the **National Cyber Strategy**, lays out the specific controls for maintaining the integrity and security of sensitive information in these systems.

4. Promoting a Strong Incident Response Framework

Incident response is another key area addressed. Both strategies stress the need for federal and state agencies to have robust response protocols in place to detect, mitigate, and recover from cyberattacks. In election systems, this translates to ensuring that there are plans to deal with system compromises, including breaches in voter registration databases or electronic poll books, preventing further damage, and restoring system integrity quickly.

5. Strengthening Deterrence and Accountability

The **Cyber Deterrence Initiative**, which is a part of the **National Cyber Strategy**, focuses on holding adversaries accountable for cyberattacks. This is particularly relevant to elections, where the risk of foreign interference is high. The strategy outlines steps to attribute attacks, apply diplomatic and legal consequences, and deter future interference attempts.

6. Federal and State Collaboration

Both strategies foster collaboration between **federal, state, and local governments**. For elections, this is crucial, as state and local governments are on the front lines of managing election infrastructure. The **National Cyber Strategy** encourages a united front, ensuring that states receive the support they need in terms of **technical assistance**, **best practices**, and **federal resources** to secure their election systems.

7. Public-Private Partnerships

The Trump administration's policies encouraged **public-private partnerships** to enhance the resilience of critical infrastructure. For election systems, this meant that vendors, security experts, and government entities collaborated to improve security measures across all election technologies, from voting machines to backend databases.

Strengthening National Election Security

The **National Cyber Strategy** and **Trump administration's cybersecurity policies** created a fortified approach to protecting the nation's election systems. Through centralizing cybersecurity management, securing supply chains, promoting continuous monitoring, and establishing incident response protocols, these strategies directly strengthened the integrity of election systems against emerging threats. The emphasis on collaboration, deterrence, and public-private partnerships ensures a comprehensive defense, making it difficult for adversaries to undermine U.S. democratic processes.

The **National Cyber Strategy** and related federal cybersecurity initiatives have provided critical frameworks to secure U.S. infrastructure, particularly focusing on election systems as key components of national security. This analysis integrates the essential elements from both the strategy and its practical applications to safeguard election systems against emerging cyber threats.

1. Strategic Focus on Critical Infrastructure

The **National Cyber Strategy** recognizes election systems as part of the **critical infrastructure** of the United States. This designation emphasizes the high priority placed on securing systems that protect democratic processes. Election systems, including voter registration databases, voting machines, and tallying systems, fall under the protection initiatives driven by this strategy. The strategy focuses on:

- **Proactive Threat Defense**: Strengthening election systems to withstand cyberattacks through continuous monitoring, real-time detection, and response capabilities.
- **Resilience Building**: Enhancing the ability of these systems to recover quickly from cyber incidents, ensuring that elections are not disrupted or compromised.

2. Federal Leadership and Coordination

The strategy establishes clear roles for **federal leadership**, particularly through agencies like the **Cybersecurity and Infrastructure Security Agency (CISA)** under the **Department of Homeland Security (DHS)**. These agencies provide state and local election officials with resources, including:

- **Threat Intelligence Sharing**: Real-time sharing of cyber threat intelligence between federal agencies and local election bodies.
- **Technical Assistance**: Direct support for securing election infrastructure, such as guidance on implementing the **NIST.SP.800-53** security controls.

By fostering **collaborative cybersecurity efforts** across all levels of government, the strategy ensures that vulnerabilities in state and local election systems are addressed with the same rigor as those in federal systems.

3. Application of NIST Standards to Election Systems

The application of the **NIST.SP.800-53** standards is crucial for election security. The **National Cyber Strategy** ties into these standards by ensuring that election systems comply with federally mandated controls. The controls cover key areas such as:

- **Access Control (AC)**: Ensuring that only authorized personnel can access sensitive election data, which protects voter databases from unauthorized changes or breaches.
- **System and Information Integrity (SI)**: Protecting election systems from malware, tampering, or data corruption, ensuring that both voter information and election results are safeguarded against cyber threats.

The **800-53A checklist** is particularly critical in assessing whether election systems meet these mandatory requirements. By conducting assessments against this comprehensive checklist, election officials can validate that their systems are secure and resilient against cyberattacks.

4. Incident Response and Cyber Deterrence

A key feature of the strategy is its focus on **incident response** and **deterrence**. Election systems are at risk from cyberattacks, both from foreign adversaries and domestic actors. The strategy provides:

- **Preparedness Measures**: Ensuring that states have robust incident response plans in place to address any cyberattack, minimizing potential disruptions during election periods.
- **Cyber Deterrence**: Establishing consequences for adversarial actions in cyberspace, deterring malicious actors from attempting to disrupt or interfere with U.S. elections.

This focus on both defense and response ensures that election systems are not only protected but can also recover quickly from cyber incidents, maintaining the integrity of the election process.

5. Enhancing Transparency and Public Trust

The strategy also emphasizes the importance of transparency in securing elections. By providing tools and support for states to **audit** and **verify** the integrity of their election systems, the strategy works to build public trust in the election process. Transparent, secure systems give the public confidence that election results are accurate and free from manipulation.

The **National Cyber Strategy**, combined with the application of **NIST standards**, provides a robust, layered defense for U.S. election systems. It ensures proactive protection, rapid incident response, and collaborative efforts across federal, state, and local levels to safeguard democratic processes from cyber threats. These efforts enhance resilience, transparency, and public trust in

election systems, ensuring that U.S. elections remain secure in an increasingly complex cyber environment.

Transparency and the Role of Cast Vote Records (CVRs)

Cast Vote Records are integral to election transparency. They provide anonymized, detailed records of individual votes cast in an election, without revealing voters' identities. These records enable **independent audits**, ensuring that votes were counted correctly and verifying the integrity of the election.

Impact on Transparency:

The **National Cyber Strategy** and **NIST guidelines** both emphasize transparency as a fundamental component of election security. Here's how CVRs fit into that:

- **Audit and Accountability (AU)**: In the **NIST.SP.800-53** framework, transparency comes from clear and auditable records. CVRs are critical because they allow third-party verification of the voting process, reinforcing confidence that the results were accurate. Banning access to CVRs directly violates this principle, making it impossible for external auditors or the public to verify election results.
- **Public Trust**: Transparency is what builds public trust in election systems. If CVRs are restricted, voters have no way to confirm whether their votes were counted as intended. This restriction creates an environment ripe for **mistrust** and **suspicion** because it blocks one of the primary tools used to verify election outcomes independently.

Violation of Legal and Policy Requirements

The **National Cyber Strategy** and other federal cybersecurity frameworks impose obligations on election systems to maintain a level of transparency, accountability, and audit-ability. By blocking access to CVRs, officials may be violating both the **spirit** and **letter** of federal mandates.

Legal Implications:

- **Freedom of Information and Public Records**: Many states have public records laws that mandate transparency in government processes, including elections. While some sensitive data (e.g., voter identities) is rightfully protected, **CVRs** are anonymized and should fall under the scope of public records that must be disclosed for accountability purposes. Denying access to these records could be a violation of these transparency laws.
- **Compliance with Federal Standards**: Election systems, particularly those using federal funds or tied to federal systems, are required to adhere to **NIST standards** (like **SP.800-53**) under the **Federal Information Security Modernization Act (FISMA)**. These standards emphasize the need for audit trails and transparency to ensure integrity and trust. The decision to block CVRs may be seen as non-compliance with these standards.
- **Potential Grounds for Legal Action**: Blocking access to CVRs could open election officials to legal scrutiny. If audits are prohibited due to the banning of CVRs, it might be argued that these officials are **interfering with the audit-ability** of elections, potentially creating grounds for legal action, including:
    - **Violation of state public records laws**.

- **Non-compliance with federal cybersecurity mandates** (e.g., **FISMA, NIST** standards).
- **Obstruction of transparency and accountability**, which could be seen as intentional malfeasance or negligence.

Security Concerns and Misconceptions

One reason officials cite for banning CVRs is the concern that they could be used to undermine voter privacy or security. However, under **NIST's Privacy Control (PT)** standards and other guidelines, **proper anonymization of data** ensures that voter privacy is maintained while still allowing for public audits. This strikes the balance between protecting personal data and maintaining the transparency needed for audits.

Grounds for Prosecution and Accountability

Election officials may face **serious consequences** for barring access to CVRs, especially if this decision leads to **non-compliance** with federal election security mandates:

- **Negligence**: If officials knowingly prevent CVRs from being audited and this results in unresolved election discrepancies or security issues, they could be held **legally accountable** for **negligent mismanagement** of election systems.
- **Potential Legal Violations**: In cases where blocking CVRs is found to violate **state transparency laws** or federal election guidelines (e.g., obstructing federal election audits), this could lead to **litigation**, removal from office, or other legal repercussions.
- **Undermining Democratic Integrity**: If election systems are shown to be vulnerable due to lack of transparency and audit-ability, it could be argued that officials are **willfully obstructing** public oversight, which could warrant further investigation or prosecution depending on jurisdictional law.

Banning **Cast Vote Records (CVRs)** from public audits effectively **destroys transparency** and public trust in elections, which are key goals outlined in the **National Cyber Strategy** and **NIST guidelines**. Not only does this violate the principle of accountability outlined in these frameworks, but it could also potentially be **illegal** under both federal mandates and state public records laws. This decision could open election officials up to **legal consequences** for obstructing transparency, failing to comply with federal cybersecurity guidelines, and undermining the public's ability to audit election processes.

EO 14028 and its Connection to EO 13800

EO 14028 outlines a national cybersecurity policy, addressing urgent vulnerabilities within the private and public sectors. It calls for a comprehensive approach to cyber incident prevention, detection, and response, emphasizing partnerships with the private sector and setting a heightened federal standard. This order acknowledges the ***increasingly sophisticated cyber threats and reinforces that protecting critical infrastructure, including elections, is essential to national security and economic stability.***

- **Alignment with EO 13800**: **EO 13800**, issued by President Trump in 2017, initially categorized cybersecurity for federal networks and critical infrastructure as a requirement

for national defense. **EO 14028** builds on this by ***enhancing requirements and accountability mechanisms, insisting on a proactive and preventive approach, and establishing cybersecurity as integral to both federal and state-level operations within critical infrastructure sectors.***

EO 14028 ***mandates*** the use of **NIST cybersecurity standards**, specifically ***requiring agencies to meet or exceed NIST SP 800-53 and SP 800-171 standards, which EO 13800 also supported.*** These frameworks focus on **risk assessment, access control, audit and accountability, and incident response**, all critical to the protection of federal and critical infrastructure systems.

- **NIST SP 800-53 and SP 800-171 Integration**: **EO 14028** requires federal agencies and their contractors to ***implement and adhere to these NIST standards***, applying them to all *cloud-based, on-premises, and hybrid environments*. ***This move brings election infrastructure, under the critical infrastructure category, into alignment with federal cybersecurity frameworks, mandating the same level of protection expected in other critical infrastructure sectors.***
- **Zero Trust Architecture**: **EO 14028** accelerates the adoption of *Zero Trust Architecture*, promoting a model that assumes network compromise is inevitable. This aligns with **EO 13800's** direction toward enhanced resilience and layered defenses, pushing agencies and critical infrastructure operators to ***continually verify system integrity and restrict access to minimize security risks.***

EO 14028 mandates the implementation of ***Endpoint Detection and Response (EDR)*** across federal networks to support *active threat hunting, incident response, and real-time monitoring*, thus enhancing situational awareness across critical infrastructure.

- **Integration with NIST Standards and EO 13800**: **EDR** complements **NIST's** risk management framework and strengthens the continuous monitoring that **EO 13800** recommended. By embedding these tools in both federal and critical infrastructure systems, the government enforces **EO 13800's** directive to adopt state-of-the-art cybersecurity tools to prevent and respond to cyber incidents promptly.

Reinforcement of EO 13800 by EO 14028 in Election Security and Accountability to NIST Standards

Supply Chain Security and the Software Bill of Materials (SBOM)

EO 14028 introduces strict guidelines for securing the software supply chain, requiring federal agencies to obtain a **Software Bill of Materials (SBOM)**. This transparency ensures that agencies can track all software components, including open-source and third-party code, which is critical to maintaining system integrity.

- **Critical Software Security**: The order demands that **NIST** develop criteria for "critical software," which would include election infrastructure software, requiring that vendors adhere to high standards of transparency and security.
- **Federal Law Accountability**: This mandate holds contractors accountable to federal standards, requiring full transparency and conformance with **NIST's** guidelines to operate

within federal and state networks. In effect, **EO 14028** enforces **EO 13800's** goal of ensuring that critical infrastructure, including elections, meets strict federal cybersecurity standards.

Log Management and Incident Reporting Requirements

EO 14028 compels agencies to improve logging and data retention for cybersecurity incidents, allowing the federal government to track and respond to threats effectively.

- **Audit and Accountability**: Logging is critical to audit and accountability, a key area of **NIST SP 800-53** and **SP 800-171**. **EO 14028's** logging requirement enforces adherence to these frameworks, ensuring that incident response teams have the necessary data to investigate and mitigate cybersecurity incidents effectively.
- **Implications for Election Security**: By establishing standardized logging requirements, **EO 14028** supports **EO 13800's** objectives to enforce federal standards across critical sectors, improving visibility into election security incidents and ensuring accountability in compliance reporting.

Federal Enforcement and Reinforcement under the Biden Administration

President Biden's administration has ***reinforced*** **EO 13800's** ***directives*** through **EO 14028** by emphasizing strict compliance with **NIST cybersecurity frameworks**, which are now non-negotiable for all federal agencies and their contractors. **EO 14028** ***obligates agencies to remove barriers that prevent information sharing about cybersecurity threats and incidents***, an initiative first proposed under **EO 13800**. By doing so, **EO 14028** ***enhances transparency and incident reporting across all critical infrastructure, including election systems.***

- **Executive Alignment with EO 13800**: Biden's **EO 14028** validates **EO 13800's** approach to secure federal and state-operated critical infrastructure, specifically election security. This reinforces the ***requirement that NIST standards apply universally to all cybersecurity operations within critical infrastructure.***
- **Coordination with Federal Agencies**: **EO 14028** mandates coordination with **CISA**, the **NSA, FBI**, and **OMB**, which are essential in enforcing **NIST**-based standards, and underscores federal responsibility in protecting state-managed critical infrastructure, including elections, under the ***cybersecurity frameworks outlined in EO 13800.***

EO 14028 as an Extension of EO 13800 and its Implications for Election and Critical Infrastructure Security

EO 14028 builds directly on **EO 13800** by enhancing cybersecurity accountability, transparency, and incident response measures within critical infrastructure. This order ***enforces federal law compliance through the adoption of NIST standards across critical sectors, embedding federal security expectations into the software and operational processes of contractors and federal agencies alike.***

As a successor to EO 13800, EO 14028 holds contractors and state agencies accountable to federal cybersecurity standards and formalizes these standards as a legal requirement across

critical infrastructure, election systems included. This alignment of EO 14028 with EO 13800 solidifies the federal government's stance on enforcing cybersecurity standards, creating a robust legal and procedural foundation for national resilience against cyber threats.

The Obama Administration's Foundational Influence on Federalizing Election Infrastructure

The Obama administration's approach to federal oversight of election security was unprecedented in scope, marked by a clear strategy to centralize control over the nation's electoral infrastructure. Through targeted executive orders, legislative actions, and the strategic use of federal agencies, the administration set the stage for federal overreach that has since reshaped the boundaries of state sovereignty in managing elections. Examined herein are the Obama administration's actions—including its surveillance of the **Trump** transition team—and illustrates how these measures laid the groundwork for the cybersecurity and administrative apparatus controlling elections today, ultimately revealing a significant intent to undermine election transparency and secure federal influence over the electoral process.

In the final months of Obama's presidency, federal agencies initiated extensive surveillance operations under the pretext of national security. Investigations by the **FBI** into alleged connections between **Trump** campaign members and Russian officials were conducted using **Foreign Intelligence Surveillance Act (FISA)** warrants. Surveillance extended to various associates within **Trump's** campaign and transition team, including **Carter Page**, through **FISA**-authorized monitoring.

The **FISA** Controversy: Later investigations uncovered that the **FISA** applications used to justify this surveillance contained numerous errors and omissions, leading to criticisms that this surveillance was politically motivated. Although the **Department of Justice's Inspector General** reported that the **FBI** mishandled its **FISA** applications, it raised broader concerns about the Obama administration's potential misuse of intelligence capabilities to undermine a political rival. This targeting of **Trump's** team indicated a deliberate intent to weaken the incoming administration's effectiveness and legitimacy, raising unprecedented challenges for the **Trump** administration to govern independently.

The Impact on the **Trump** Administration: The publicized investigations placed the incoming administration under an immediate cloud of suspicion, creating obstacles for staffing, policy implementation, and coordination with federal agencies. The surveillance of **Trump's** team added a layer of friction with intelligence agencies, reinforcing a distrustful environment that hindered **Trump's** administration's capacity to address critical national issues, including election infrastructure reform.]

The Obama administration's series of executive orders, particularly **EO 13636** on cybersecurity and **PPD-21** on critical infrastructure, were instrumental in expanding **DHS's** influence over election infrastructure:

Executive Order 13636 and PPD-21: These orders gave **DHS** new authority to secure sectors labeled as critical infrastructure, enabling it to determine which sectors warranted federal oversight.

Although elections were not initially designated as critical infrastructure, these actions gave **DHS** a pathway to extend control over election systems in response to perceived threats.

The January 2017 Critical Infrastructure Designation: In one of his final acts, **Secretary of Homeland Security Jeh Johnson** designated election infrastructure as critical infrastructure, positioning it under **DHS's** control. The timing of this designation, days before **Trump's** inauguration, indicated an urgency to secure federal jurisdiction over elections before the incoming administration could take office, shaping the trajectory of federal oversight under **Trump.**

In addition to direct actions through executive orders, the Obama administration leveraged media influence through the **Smith-Mundt Modernization Act of 2012**, which permitted federal agencies to use domestic media for public diplomacy purposes. Originally intended for foreign audiences, the modernization of **Smith-Mundt** enabled the administration to shape public opinion on issues deemed critical to national security, including election security.

Promoting Federal Control as Necessary for Security: With media influence, the Obama administration and subsequent federal agencies were able to frame the critical infrastructure designation of election systems as a necessary response to cybersecurity threats. This narrative fostered public support for federal oversight, portraying state-controlled election systems as potentially vulnerable, and discouraging opposition from state officials.

Suppressing Dissenting Voices on Election Sovereignty: By setting the public narrative through federal influence in media, alternative viewpoints on election sovereignty were overshadowed. Media campaigns discouraged scrutiny of **DHS's** and, later, **CISA's** expanding influence over state-run elections, making it politically challenging for states to question the federal narrative without facing public backlash.

The Obama administration's executive actions and surveillance measures exemplify a coordinated strategy to build an administrative state that would maintain influence over election infrastructure beyond his presidency. By structuring federal agencies to control cybersecurity policies, including those over election systems, Obama's legacy embedded the foundation for an advisory apparatus with an outsized influence over state-run elections.

The Obama administration's foundational influence over election infrastructure, exemplified by *executive actions, surveillance activities, and media control*, represents a concerted effort to ***centralize election security under federal jurisdiction.*** These actions established an ***administrative state with substantial autonomy over election infrastructure, laying the groundwork for today's opaque and federally dominated election system.*** By strategically positioning **DHS** and changing the roles of **CISA** under the Biden Administration (Obama's VP) as gatekeepers of election cybersecurity and framing federal oversight as a security necessity, ***Obama's administration initiated a shift away from state sovereignty and transparency in elections.***

The legacy of these actions endures, posing a clear and present danger to the integrity of U.S. elections and raising critical questions about the balance of power between state authority and federal control. This systemic shift toward federalized elections represents an ongoing threat to democratic accountability and the decentralized governance that has historically protected the nation's electoral process.

Federalization of Election Infrastructure and the Path Forward

The progressive centralization of election security oversight in the United States, originating under the Obama administration, has created a powerful administrative state apparatus capable of ***influencing, if not directly controlling, the electoral process.*** Beginning with critical infrastructure executive orders and culminating in the designation of election infrastructure as critical in 2017, these measures embedded election systems within the **Department of Homeland Security's** purview. ***As an advisory agency created within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) has leveraged its role to advise states in ways that increasingly resemble federal mandates, influencing states to adopt practices under the guise of "best practices" that bypass true regulatory processes.***

CISA's influence has ***extended beyond mere advisories***; it has actively encouraged states to ***implement security measures that restrict public access to critical election information.*** This ***advisory influence*** has muddied the *transparency* **mandated by Executive Order 13800** and the **NIST Cybersecurity Framework**, both of which were designed to ensure that federal election security standards were *met, audited, and open to public scrutiny.* However, through its guidance, **CISA** has effectively created a ***layer of controlled access to election data, restricting transparency and undermining public confidence in electoral integrity.***

Obama's Administrative Foundations: The Obama administration's use of executive power and advisory agency influence laid the groundwork for expanded federal authority in election systems, affecting the nation's previous decentralization of election oversight.

The Role of **DHS** and **CISA**: **DHS's** foundational directives enabled a shift from state-controlled election systems to a federally influenced infrastructure. **CISA's** subsequent **"advisory"** role allowed it to subtly yet powerfully ***affect state policies without regulatory authority, encouraging restrictions on public record access and transparency.***

Real-World Implications and Case Studies: The case of officials like **Tina Peters** underscores the consequences for those who attempt to align their practices with ***federal retention standards***, only to face backlash from ***state laws shaped by CISA's guidance.***

National Security Risks: Non-compliance with **NIST** and federal standards across states presents ***significant cybersecurity vulnerabilities***. This broad systemic issue threatens not only elections but also ***interconnected sectors, leaving critical infrastructure susceptible to exploitation.***

Current Federal Actions: **CISA's** upcoming nationwide cybersecurity exercises exemplify the current risks posed by ***advisory agencies conducting pseudo-regulatory activities.*** Such exercises, particularly around election time, highlight a ***problematic overreach that could interfere with election security and create confusion in the event of a true cyber threat.***

Through this evolution from state oversight to federal advisories with de facto authority, the Obama administration set in motion a series of changes that allowed subsequent administrations to exert control over election security. The Trump administration's attempt to restore

transparency through EO 13800 represented a significant effort to reassert federal law in election security."However, without stringent enforcement or mandatory third-party assessments, compliance with EO 13800 and NIST frameworks—federally mandated by law—has been inconsistently followed, with many states prioritizing CISA's advisories over legally binding federal standards. This reliance on CISA's guidance has enabled states to overlook mandatory transparency, auditability, and security protocols, further compounding national vulnerabilities in election infrastructure."

Given the covert weaponized malware threats targeting critical infrastructure and the overreach by **DHS** and **CISA** into election systems through cybersecurity advisories, a fundamental overhaul of our election process is essential. ***Returning to paper ballots, counted in-person with voter ID, at the precinct level is the only way to restore the security and integrity of U.S. elections.*** The vulnerabilities inherent in voting machines make them ill-suited for the sophisticated cyber threats of today; ***they must be dismantled and repurposed as scrap, as they offer no reliable defense.***

Even if states adhered strictly to federal laws and the **NIST cybersecurity standards,** these systems would still fall short of protecting our elections from current cyber threats. Complex solutions like blockchain or encryption might seem promising but present only temporary barriers before they, too, are compromised. ***A truly secure voting system must be fully offline, with physical ballots and voter registration lists managed transparently and locally, away from digital interference.***

Key Measures for a Resilient, Transparent Voting System:

In-Person, Paper Ballot Voting: Voting should be conducted in person, using paper ballots at the local precinct level. Voter ID requirements, checked against pre-printed paper rosters, ensure each ballot is associated with a verified individual. Only those with legitimate reasons should be allowed to request absentee ballots, and these should be approved by local authorities to prevent misuse.

One-Day National Voting Holiday: Election Day should be a national holiday, enabling every eligible American to exercise their right to vote without compromising work or personal responsibilities. Local governments should provide free transportation to voting centers for those who need it to prevent any disenfranchisement, ensuring accessible voting for all.

Eliminating Unused Ballots: Only precincts should request the specific number of ballots required for registered voters on their rolls. Ballots should be printed only for those registered by a designated cutoff date well before Election Day. This eliminates excess ballots and curtails opportunities for fraud. Voters would sign a pre-printed roster upon arrival, receive a ballot, and fill it out in private booths.

Secure, Local Ballot Collection and Counting: Each precinct should manage its ballots on Election Day, depositing them into secure, sealed ballot boxes. Precincts, ideally no larger than 1,500 people, would count ballots immediately upon the close of polls, with results verified and open to observation by community members under the supervision of local law enforcement.

Direct Reporting and Public Verification: Results should be posted publicly in the precinct and reported directly to the county, then to the state. The process is rapid, yielding results by the next morning, while the transparency and localized nature reduce costs significantly across every state.

By reverting to a fundamentally secure, offline, and transparent voting system, we can restore the integrity of the electoral process, ensuring that every vote is accurately counted without interference or manipulation. This path represents not only the most secure means to protect our elections but also the most direct and cost-effective way to safeguard American democracy against the escalating cyber threats of today.

LONG LIVE THE REPUBLIC!