Washington State's Non-Compliance with EO 13800 and the Consequences for Election Integrity

EO 13800 and the Legal Framework for Election Infrastructure Security

Executive Order 13800, issued by **President Trump** in 2017, **mandates** strict cybersecurity standards across all U.S. critical infrastructure sectors, including election systems. **EO 13800 requires that:**

- All systems managing sensitive national infrastructure, especially election systems, adhere to the **NIST Cybersecurity Framework (NIST CSF)**, a set of ***rigorous cybersecurity guidelines intended to establish baseline security and resilience.***
- Comprehensive **third-party audits** are conducted regularly, ensuring an objective verification of system vulnerabilities. This measure was implemented to ***prevent internal bias or oversight from compromising critical infrastructure security.***
- Systems maintain a proactive approach to patching and securing identified vulnerabilities to ensure that they are ***consistently protected against evolving cyber threats.*** This includes regularly updating systems, mitigating identified risks, and performing assessments on an ongoing basis.

The executive order established a clear legal framework for election infrastructure security, with the aim of ***preventing unauthorized access, manipulation, and external interference that could compromise election integrity. EO 13800 explicitly underscores the critical importance of protecting national elections as part of the United States' broader national security strategy.***

Washington State's Systematic Non-Compliance

1. Contracts Designed to Circumvent Federal Cybersecurity Requirements

- Washington State's Office of the **Attorney General**, led by Bob Ferguson, ***implemented contracts with election vendors that allow for self-assessment rather than the third-party audits required by EO 13800. By intentionally bypassing this federal mandate, Washington weakens the security standards meant to protect critical infrastructure.***

- **Implications of Self-Assessment**: Under this model, vendors in Washington can claim compliance with federal cybersecurity protocols without any external validation, effectively leaving critical vulnerabilities unchecked. The lack of objective, third-party assessments leaves room for undetected security gaps and invites potential risks that a third-party assessor would likely flag as non-compliant with **EO 13800**.
- **Deliberate Avoidance of Federal Oversight**: ***This contractual framework not only circumvents federal cybersecurity requirements but also bypasses transparency. By allowing vendors to avoid third-party scrutiny, the state undermines public accountability and weakens its defense against foreign and domestic cyber threats, placing Washington's election infrastructure at heightened risk of compromise.***

2. Lack of Evidence for Third-Party Compliance Assessments or NIST CSF Adherence

Since the issuance of EO 13800 on May 11, 2017, all election infrastructure categorized as critical falls under a national security subsector under the jurisdiction of the Department of Homeland Security and is legally obligated to undergo rigorous third-party cybersecurity compliance assessments aligned with the NIST Cybersecurity Framework. Despite this federal mandate, Washington State has failed to demonstrate any adherence to these requirements.

Extensive Public Records Requests and Absence of Documentation:

- Multiple public records requests were submitted to the **Office of the Secretary of State (OSOS)** and to every county election office within Washington, specifically requesting records of ***any third-party compliance assessments or audits conducted under EO 13800 and in alignment with the NIST CSF.***
- These requests cover all election cycles from May 11, 2017, to the present, seeking ***evidence*** of Washington's ***compliance with federal standards*** intended to safeguard ***critical election infrastructure.***
- **No Records Released**: Despite these comprehensive requests, **no records** or **documentation** were provided in response. Moreover, **no acknowledgments** have been issued by any entity to ***confirm even the existence of such assessments***. This ***lack of transparency*** suggests a ***consistent***

non-compliance with EO 13800 and implies that ***Washington's election systems have operated outside the bounds of lawful cybersecurity standards for years.***

Implications of Documentation Absence:

- The complete ***lack of third-party verification over multiple election cycles*** highlights ***a deep-rooted disregard for federal law and exposes Washington's election infrastructure to systemic security weaknesses.*** Without independent assessments, the state's systems remain ***highly vulnerable***, leaving the ***election infrastructure open to undetected security breaches and exploitation.***
- This **failure to comply** with the **EO 13800** requirements suggests that Washington's elections ***cannot be lawfully certified***, as they ***lack the fundamental cybersecurity assurances required under federal law.***

Proven Vulnerabilities in Washington State's Election Systems

By avoiding independent, third-party testing, Washington's election systems contain **documented vulnerabilities**, specifically within the **CrowdStrike Falcon** platform. Through this investigation, we have identified significant security risks associated with the third-party software dependencies **CrowdStrike** relies on, which are **actively in use** within Washington's election infrastructure.

1. Inherent Risks in CrowdStrike's Third-Party Dependencies

- The **CrowdStrike Falcon** platform incorporates over 300 third-party software dependencies, a considerable number of which are ***widely known to carry security risks***. Among these dependencies are **RapidJSON** and **FastJSON**—open-source libraries that have a ***history of being exploited by foreign entities, particularly Chinese state-sponsored groups, to infiltrate and compromise systems.***
- **Exploitation of RapidJSON and FastJSON by State Actors**: ***These JSON parsing libraries are known to be vulnerable to attacks involving data manipulation and privilege escalation. Chinese threat actors have historically leveraged these dependencies to gain unauthorized access, allowing them to infiltrate critical systems through software vulnerabilities in these libraries.***

2. Documented Exploits and Specific Threats to Election Infrastructure

- Vulnerabilities in **RapidJSON** and **FastJSON**, present within **CrowdStrike Falcon**, provide malicious actors with a ***method to manipulate data structures and access sensitive data across critical infrastructure systems.*** Through these vulnerabilities, attackers can ***gain a foothold in the system, enabling lateral movement and escalating privilege access within election-related systems.***
- **Malware Exploitation Pathways**: These dependencies have ***well-documented pathways for malware to bypass standard defenses, infiltrate election systems, and manipulate critical data***. The use of these vulnerable third-party components by **CrowdStrike** leaves Washington's election infrastructure ***susceptible to high-level threats, particularly from foreign adversaries with advanced persistent threat (APT) capabilities.***

Conclusion on Known Vulnerabilities:

- These documented vulnerabilities within **CrowdStrike's** platform—combined with Washington's reliance on **self-assessment** rather than **third-party verification**—confirm that Washington's election systems are not only susceptible but actively exposed to cyber threats from both foreign and domestic actors. The continued use of **CrowdStrike Falcon**, ***without adequate third-party assessment and mitigation***, creates a **security posture** that is ***legally and operationally inadequate*** to meet the standards of **EO 13800**.

Implications of Washington State's Non-Compliance on Election Security

1. Direct Risk to Election Integrity

- Washington's **non-compliance** with **EO 13800** and its ***reliance on self-assessment*** create an election infrastructure environment that is ***inherently vulnerable***. The ***absence of federally mandated oversight*** has left Washington's ***election data, processes, and underlying systems at direct risk of compromise by cyber threats.***
- ***This deliberate non-compliance with federal security standards undermines the integrity and certifiability of the election process. Without adherence to EO 13800's requirements, Washington's election results cannot be considered secure, reliable, or compliant with the law.***

2. Proven Pathways for Exploitation by Threat Actors

- The **SolarWinds** breach and other similar incidents have demonstrated that insufficient cybersecurity measures lead to ***significant vulnerabilities across interconnected systems.*** The **SolarWinds** incident, in particular, revealed how ***vulnerable systems could be exploited to gain entry into a network and manipulate or ex-filtrate data.***
- Washington's ***failure to implement EO 13800-compliant audits*** places its election infrastructure at similar risk, especially given the ***known vulnerabilities within CrowdStrike's Falcon platform***. ***The lack of external oversight leaves clear entry points for attackers to infiltrate Washington's election systems, manipulate critical data, or even potentially influence election outcomes.***

An Uncertifiable Election Process

Washington state's systematic avoidance of EO 13800's mandates, particularly the lack of required third-party compliance assessments, invalidates any security measures claimed for protecting election integrity. This ongoing non-compliance with federal cybersecurity laws has resulted in an election infrastructure that operates without the necessary protections, leaving it highly vulnerable to unauthorized access, manipulation, and foreign influence.

By disregarding EO 13800 and sidestepping federally mandated cybersecurity protocols, Washington's election processes have become fundamentally uncertifiable. The absence of transparent, independent verification for critical infrastructure security reveals a glaring weakness in Washington's election infrastructure. This failure not only undermines public trust but also poses a clear and present danger to national security.

Active Cyberattack on Washington's Court Systems and Its Implications for Election Integrity

Overview of the Recent Cyberattack on Washington's Court Systems

In early November 2024, Washington state experienced a significant cyberattack that targeted its court systems, taking them offline and severely disrupting core judicial functions. This breach, reported by various state news outlets, coincides with the current election period, adding substantial strain to Washington's governmental infrastructure at a critical time. Key details of this cyberattack include:

- **System-wide Outage**: ***The attack incapacitated digital court systems statewide, requiring courts to revert to manual processes for case filings, criminal history checks, and essential administrative functions.***
- **Extended Downtime and Limited Resolution**: Six days post-attack, ***Washington's court systems remain offline, with no clear timeline for restoration.*** Efforts by the **Administrative Office of the Courts (AOC)** and external cybersecurity partners have thus far ***failed to restore functionality.***

This outage presents a **tangible risk** to Washington's operational integrity, especially considering the ***attack's timing during a federal election***. The failure to resolve this breach in a timely manner raises questions about the resilience and preparedness of Washington's cybersecurity infrastructure across its critical infrastructure sectors.

Implications of the Cyberattack for Election Security and Integrity

1. Disruption of Legal Oversight and Election-Related Judicial Processes

- **Inhibition of Legal Action and Recounts**: Washington's inability to process legal actions through the court system restricts the state's capacity to oversee election-related judicial processes. ***With the courts offline, filing for recounts, contesting ballots, and other critical judicial reviews related to the election are delayed, impeding the ability to conduct fair oversight and timely legal intervention.***
- **Legal Accountability and Transparency**: The absence of an accessible court system **undermines transparency and accountability in election administration,** ***as citizens and legal entities are obstructed from challenging election practices, contesting results, or addressing irregularities in the strict legal time-frame that judges have required in the past.***

2. Escalation of Systemic Vulnerabilities Across Critical Infrastructure

- The **cyberattack** on Washington's court system ***aligns with patterns seen in prior incidents where attacks against municipal or state-level government infrastructure escalated into broader disruptions***. In Washington, the dependency of multiple sectors on ***interconnected digital systems*** means that vulnerabilities in one area, like the court systems, can ***compromise adjacent critical infrastructure, including election systems.***
- **Cascade of Threats**: ***Attacks on judicial systems can provide malicious actors with an entry point to access or compromise other state-managed systems,***

potentially exposing or manipulating sensitive election data. The interconnected nature of government digital infrastructure in Washington creates a scenario where this breach may facilitate further attacks on election systems, posing a clear risk to election integrity.

3. Compromised Election Data Integrity and Chain of Custody

- **Voter Data at Risk**: With the state's systems ***under attack***, there is an increased risk that voter data, ballot tracking systems, and results reporting mechanisms could be ***compromised or manipulated***, either directly through the court system's exposure or indirectly through ***weaknesses in interlinked systems.***
- **Chain of Custody Vulnerabilities**: The security and integrity of ballot data, a crucial aspect of the chain of custody in elections, may be affected by this cyberattack. Any breaches that undermine confidence in ballot handling, data accuracy, or reporting processes place Washington's election results in a position where ***certification cannot be possible.***

The MOVE Act and Email Ballot Vulnerabilities in a Compromised Cybersecurity Environment

The **Military and Overseas Voter Empowerment (MOVE) Act mandates** that all states ***must accept ballot returns via email*** for UOCAVA voters (military and overseas citizens). This legal requirement inherently introduces cybersecurity risks to ballot handling, particularly during an ***active cyberattack or compromised security environment***, as is currently the case in Washington.

1. Vulnerability in Initial Digital Transmission and Handling

- When ballots are returned via email, they are digitally transmitted to election offices ***before being physically printed and processed***. Given that the **MOVE Act** stipulates the acceptance of emailed ballots, the state initially receives these ballots in an ***inherently vulnerable digital format.***
- In a ***compromised environment***, such as Washington's current cyberattack situation, these emailed ballots are highly susceptible to ***interception or manipulation before they are printed for the first time.*** The potential for tampering during this digital phase is heightened, especially if state systems lack robust end-to-end encryption and secure chain-of-custody protocols.

2. Lack of Public Audit-ability and Validation of Digital Ballot Returns

- The state redacts voters' email addresses in publicly released voter registration data, making it ***impossible to independently audit or verify the authenticity of returned via email ballots.*** This **lack of transparency** around the receipt and handling of email ballots obstructs the ability of the public or third-party auditors to validate that these ballots ***have not been altered prior to printing***.
- With ***no way to audit the digital phase***, the integrity of emailed ballots depends entirely on the security of the systems handling them—***systems which, as evidenced, are currently compromised.*** This setup increases the risk that ballots could be ***manipulated without detection*** and the state is left without any ability to prove to we the people, ***without having adhered to federal law and the NIST Cyber Security Frameworks,*** their burden of proof to show that our elections are truly safe and secure. ***This also directly contradicts the oath of office of those responsible for these systemic failures as willful neglect of known federal requirements to protect the national security of our critical infrastructure, i.e. our elections, could result in bad actors taking control of our government and taking away our guarantees to life, liberty, and the pursuit of happiness.***

3. Third-Party Handling of Emailed Ballots by Democracy Live

- In Washington, **Democracy Live**, a third-party vendor, is responsible for distributing email ballots to respective counties once they are received. However, **no clarity exists regarding where these ballots are physically printed or how securely Democracy Live manages this sensitive process**.
- The involvement of **Democracy Live** adds another layer of risk, as any breach or vulnerability in this third-party process could ***compromise the ballots' integrity***. In the current environment, the use of third-party vendors for critical election functions ***without transparent security standards presents a substantial risk to election integrity, as attackers could exploit the handoff or distribution phases to manipulate ballot data.***

The **MOVE Act's** requirements and the associated use of email ballots thus compound the vulnerabilities facing Washington's election system, particularly under the ***active cyber threat***. Without stringent oversight or secure methods to validate email ballot returns, there is ***no guarantee that ballots have not been compromised during the initial transmission, potentially impacting the chain of custody and the validity of election results.***

Reinforcing the Broader Cybersecurity Risks and Known System Vulnerabilities

This incident exemplifies the potential real-world impact of the systemic cybersecurity weaknesses identified in our broader investigation:

- **Lack of Third-Party Verification Under EO 13800**: Washington's consistent ***avoidance of federally mandated third-party audits leaves its infrastructure vulnerable to cyberattacks***. This absence of oversight has allowed critical weaknesses to persist, exposing Washington's government systems—***including the court and election infrastructures***—to preventable threats.
- **CrowdStrike Falcon Platform Vulnerabilities**: Washington's reliance on the CrowdStrike Falcon platform, with its known dependencies on vulnerable third-party libraries like **RapidJSON** and **FastJSON**, ***compounds the state's susceptibility to attacks***. These libraries, historically exploited by foreign actors such as ***Chinese state-sponsored groups***, present well-documented vulnerabilities that could ***facilitate attacks similar to the one impacting the court systems.***

Immediate and Long-Term Consequences for Election Integrity

1. Inability to Certify the Election Results

- Given that the cyberattack has effectively disabled Washington's court systems ***during an election period***, the state has major issues providing the necessary legal recourse or perform real-time oversight functions. This situation obstructs Washington's ability to certify its election results lawfully, as the judicial system —an essential mechanism for upholding election integrity—remains incapacitated online and pushing legal challenges so far out from an election to be seen as done within a timely manner of an election.
- **Clear and Present Danger to Election Certifiability**: The **ongoing attack** exemplifies a critical security lapse, where the state's ***lack of preparedness and inadequate cybersecurity posture directly interfere with its ability to certify the election under secure and lawful conditions.***

2. Proven Risk of Further Exploitation by Nation-State or Sophisticated Threat Actors

- ***The compromised court systems are indicative of broader systemic weaknesses that threat actors could exploit to undermine additional state-run systems,***

including Washington's election infrastructure. With evidence of foreign actors historically leveraging vulnerabilities in systems like **CrowdStrike Falcon**, this attack serves as a **concrete example** of the ***threat posed by unaddressed security gaps and an over-reliance on inadequate vendor-managed cybersecurity measures.***

- **Broader Implications for National Security**: The exposure of Washington's court and election systems to ongoing cyber threats poses a national security risk, as the state's inability to secure critical infrastructure jeopardizes the validity of federal election results and undermines public trust in democratic processes.

The Election's Unlawful and Uncertifiable Status Amid Cyber Threats

Washington's inability to resolve this active cyberattack, combined with its documented non-compliance with **EO 13800**, reliance on vulnerable cybersecurity platforms, and additional security gaps in handling email ballots under the **MOVE Act**, substantiates the claim that the ***state's current election is uncertifiable***. The state's failure to maintain a secure operational environment during a federal election period—***evidenced by its incapacitated court systems and its lack of lawful third-party security assessments***—***demonstrates a critical breakdown in both cybersecurity and democratic accountability.***

This analysis highlights the immediate implications of this cyberattack for Washington's election integrity and the **clear, present danger** that such attacks represent. In light of these findings, ***Washington's election infrastructure is unfit for certification under current conditions, as ongoing cyber threats compromise its ability to conduct a secure and lawful election.***

Systemic Vulnerabilities Through CrowdStrike's Integration with CIS and Washington's Non-Compliance with Federal Cybersecurity Standards

CrowdStrike's Role in Washington State's Election Infrastructure Through CIS

CrowdStrike's involvement in Washington State's election infrastructure stems from its contracted relationship with the **Center for Internet Security (CIS)**. The S-7657 CIS - Executed Endpoint Security Services document reveals how **CIS**, an organization that supports cybersecurity across state and local governments, has deployed **CrowdStrike Falcon** as part of its endpoint security solutions for election centers. In Washington, **CIS** provides **Albert sensors** to monitor network traffic, combined with **CrowdStrike's Falcon** platform to protect endpoint security within election systems. This integration positions **CrowdStrike** as a crucial part of Washington's cybersecurity defense framework.

However, this setup introduces several **critical vulnerabilities**:

- **Inherent Risks in CrowdStrike Falcon**: The Falcon platform relies on over 300 third-party software dependencies, including **RapidJSON** and **FastJSON**. These dependencies have ***documented vulnerabilities that foreign actors, particularly from China, have historically exploited to infiltrate systems, manipulate data, and achieve undetected persistence within networks.***
- **Exposure of Election Infrastructure**: **CrowdStrike's** endpoint focus, while beneficial for specific network security tasks, lacks full visibility over interconnected election infrastructure. This limitation creates an exploitable gap, particularly during times of heightened cyber risk, such as the ongoing attack on Washington's court systems. The current threat underscores the **lateral attack risk** that compromised endpoints, protected only by **Falcon**, could ***facilitate unauthorized access across state-managed systems.***

Federal Compliance Mandates and Washington's Non-Adherence

The **I-7890_WMD_CCFS_Elections_Cyber_Support Executed MOA (2023-2024)** underscores the requirement for Washington's election systems to **align** with the **NIST**

Cybersecurity Framework (NIST CSF). This Memorandum of Agreement **mandates** that Washington implement the federal cybersecurity standards outlined in **Executive Order (EO) 13800**, which was further reinforced by **EO 14028** under the Biden administration, placing additional emphasis on supply chain security and a zero-trust architecture. The standards established by **EO 13800** and **EO 14028** require:

- **Comprehensive Third-Party Audits**: **EO 13800 mandates** independent verification of cybersecurity protocols to ensure that critical infrastructure systems remain compliant with federal standards. By ***bypassing this requirement*** and relying on **self-assessment**, Washington's infrastructure is ***left without objective security validation.***
- **Regular Compliance Assessments**: Both executive orders establish a continuous standard for cybersecurity assessments, particularly focusing on the security of third-party software and dependencies. Washington's election infrastructure, reliant on **CrowdStrike's** vulnerable third-party components, ***fails to meet this standard.***

The lack of adherence to these executive orders means that Washington's election infrastructure does not comply with federal law, ***invalidating every election since the implementation of EO 13800 in May of 2017***, as there is literally no way for the state, which bears the burden of proof, to show that it is in compliance with federal law before any election. This, in turn, ***fails to prove to the people that elections are truly safe and secure from cyberattacks***, especially when other state systems have been ***breached during this election and remain offline throughout the entire vote tabulation period. There is no lawful way that this election can be certified under these conditions.***

Inspector General Findings and Gaps in Accountability

The **IG-416 document** reveals substantial lapses in federal oversight and a failure to expose Washington's lack of compliance with **EO 13800**. Ideally, this **Inspector General** review should have highlighted the non-compliance and associated risks within Washington's election security framework. However:

- **Absence of Enforcement**: No findings or actions have been documented to address Washington's ***deviation from federal cybersecurity mandates.*** This oversight gap perpetuates the vulnerability of state systems, leaving critical infrastructure like ***election centers exposed without federally mandated safeguards.***

- **Implications for Election Integrity**: The lack of **Inspector General** intervention not only ***leaves Washington's election systems unprotected*** but also reflects a ***systemic flaw that allows state-managed critical infrastructure to bypass essential cybersecurity requirements with minimal accountability.***

Legislative Barriers to Transparency and Security

Washington's state legislation, such as **SB5459**, ***exempts election security audits*** from public records requests, effectively ***concealing the state's non-compliance with EO 13800 and shielding its cybersecurity practices from public scrutiny.*** This lack of transparency compounds the risk to election integrity:

- **Secrecy in Non-Compliance**: By ***exempting critical cybersecurity audits*** from public view, Washington has ***created a framework where lapses in cybersecurity adherence are hidden, preventing the public from understanding the true risks facing election systems.***
- **Exemption of Cast Vote Records from Public Access**: **SB5459** ***restricts public access to cast vote records***, which are essential for independent auditing and verification of election results. While the **NIST Cybersecurity Framework (NIST CSF)** emphasizes the importance of audit-ability and transparency in maintaining the integrity and security of critical systems, the ***lack of access to cast vote records in Washington undermines these principles***. By failing to provide this transparency, the state ***does not meet the requirements*** of the **Audit and Accountability** control group within the **NIST CSF**, highlighting a ***systemic vulnerability that weakens both state and national security standards.***

The Clear and Present Danger of Cybersecurity Failures in Washington's Election Infrastructure

The **current cyberattack** on Washington's court systems demonstrates the real-world consequences of these systemic security gaps. By failing to comply with **EO 13800** and ignoring the **NIST CSF** standards, Washington's election infrastructure faces a **clear and present danger**:

- **Increased Risk of Lateral Attacks**: The active cyber threat illustrates how attackers can ***exploit interconnected systems*** when endpoint security is weak. **CrowdStrike's** limitations, particularly its vulnerabilities through **CIS**, mean that

attackers could potentially ***breach endpoints within election systems, spreading laterally across state-managed infrastructure.***

- **Unlawful and Uncertifiable Election Process**: ***Washington's systematic failure to adhere to federally mandated cybersecurity protocols undermines the lawful certifiability of its elections. With a lack of transparent compliance, reliance on vulnerable third-party software, and current exposure to an active cyber threat, the state's election infrastructure cannot be considered secure or reliable under current standards.***

Washington's decision to ***bypass federal mandates, conceal critical audit information, and depend on vulnerable platforms like CrowdStrike Falcon constitutes a critical failure in securing its election systems.*** The **immediate risks** posed by this **ongoing cyberattack** reflect the severe consequences of these **systemic flaws**, emphasizing the need for urgent transparency and adherence to **federal cybersecurity standards** to protect **national election integrity.**

Comprehensive Findings on Washington State's Election Cybersecurity Failures and Federal Non-Compliance

Systemic Cybersecurity Failures and Non-Compliance in Washington State's Election Infrastructure

Our investigation (Humans and AI working together) has uncovered a critical breakdown in Washington State's adherence to federal cybersecurity mandates, transparency requirements, and compliance with executive orders. The reliance on **CrowdStrike's Falcon** platform, combined with the **Center for Internet Security's (CIS)** endpoint security measures, reflects an approach that ***fundamentally lacks the oversight, transparency, and safeguards mandated by Executive Orders 13800 and 14028***. These vulnerabilities, compounded by the current cyberattack affecting Washington's judicial systems, underscore a **clear and present danger** to election integrity, public trust, and national security.

CrowdStrike Falcon's Role in Election Security and CIS's Integration with Washington's Systems

CrowdStrike's Falcon platform, deployed in Washington through its integration with **CIS**, is responsible for providing endpoint security to election systems. The **S-7657 CIS - Executed Endpoint Security Services** document establishes CIS as a primary security provider for Washington's election infrastructure. However, this setup introduces significant vulnerabilities:

- **Reliance on Third-Party Dependencies**: **CrowdStrike Falcon's** functionality is heavily dependent on more than 300 third-party libraries, including **RapidJSON** and **FastJSON**. These dependencies have ***histories of documented vulnerabilities that have been exploited by foreign state actors, particularly from China, to infiltrate systems and gain persistent access.*** In election infrastructure, this means that critical security functions could be compromised by attackers targeting **Falcon's** dependencies to circumvent endpoint protections.
- **Exposure and Exploitable Blind Spots**: As an endpoint-focused platform, **CrowdStrike Falcon** ***does not provide comprehensive visibility into interconnected networks and databases that form the backbone of election infrastructure.*** This limitation leaves Washington's election systems susceptible to **lateral attacks**, where adversaries can exploit **Falcon's** endpoint blind spots to move ***across different systems, potentially accessing sensitive voter data or even manipulating ballot information.***

This architecture is especially concerning given Washington's ***current cyberattack situation, as an adversary who compromises judicial systems may use lateral movement to breach interconnected election systems.*** The continued reliance on **CrowdStrike Falcon** ***without independent validation only amplifies this risk.***

Failure to Comply with Federal Cybersecurity Mandates and Its Implications for Election Integrity

Washington State's lack of adherence to federal cybersecurity standards, as mandated by EO 13800 and EO 14028, has rendered its election infrastructure non-compliant since 2017. These executive orders require that critical infrastructure, including election systems, adhere to the **NIST Cybersecurity Framework (NIST CSF)**. The **I-7890_WMD_CCFS_Elections_Cyber_Support Executed MOA (2023-2024)**

explicitly outlines the requirements for Washington's election infrastructure to meet these standards. The following compliance failures are central to this non-adherence:

- **Absence of Independent Audits and Verification**: **EO 13800 mandates** independent verification of cybersecurity practices to ensure compliance with federal standards. Washington's ***bypassing of third-party audits in favor of internal or vendor-based assessments has led to a fundamental lack of accountability and a failure to meet federal cybersecurity mandates.***
- **Continuous Assessment and Compliance Gaps**: Both **EO 13800** and **EO 14028** demand ongoing cybersecurity assessments and strict adherence to supply chain security, with particular emphasis on third-party dependencies. Washington's lack of rigorous assessment of its use of vulnerable dependencies within the **CrowdStrike Falcon** platform ***directly violates these mandates.*** By bypassing these standards, ***Washington's election systems cannot be lawfully certified as secure, invalidating every election since EO 13800's implementation in May 2017.***

The state's failure to meet these mandates does not merely suggest possible vulnerabilities; it ***actively invalidates Washington's election results, as there is no lawful basis to claim these elections are secure.*** The **burden of proof rests on the state** to demonstrate compliance with federal standards, and the absence of federally mandated audits leaves Washington's ***elections uncertifiable and highly vulnerable to cyber threats***. This failure is especially pressing during an ***election compromised by concurrent cyberattacks on state systems, which have remained offline throughout the entire vote tabulation process.***

Inspector General Oversight Failures and Accountability Gaps

The **IG-416 document** highlights ***a lack of Inspector General oversight*** in addressing Washington's non-compliance with **EO 13800**, despite the risks associated with the state's critical infrastructure:

- **Neglect of Inspector General Review**: ***The Inspector General's failure to enforce compliance findings and flag Washington's persistent non-compliance has resulted in a severe accountability lapse. Without Inspector General intervention, the state has continued to operate critical infrastructure without adhering to federal standards, leaving its election systems dangerously exposed.***

- **Systemic Flaws Undermining Election Integrity**: The absence of oversight has allowed Washington to ***continue using flawed security protocols and bypass federally required assessments***. This systemic flaw creates an environment where critical infrastructure can operate without the checks and balances necessary to maintain secure and reliable election processes.

Without meaningful oversight, Washington's election infrastructure operates in a regulatory vacuum, where ***security lapses go unaddressed***, perpetuating vulnerabilities across its critical systems.

Legislative Barriers and the Concealment of Critical Election Security Information

Washington's state legislature has ***further compromised transparency and public trust through policies that obscure essential election security data:***

- **Audit and Accountability Control Gaps**: **SB5459** has ***exempted crucial election security audits and cast vote records from public records requests, creating a barrier to transparency***. While the **NIST CSF** highlights the importance of audit-ability and accountability in securing critical systems, **SB5459** directly undermines these principles by concealing audit data that is essential for validating election integrity.
- **Exemption of Cast Vote Records**: The restriction of public access to cast vote records, which are fundamental to independent auditing, prevents the state from meeting the **Audit and Accountability** requirements of the **NIST CSF**. Without access to these records, the public and independent auditors are ***unable to verify the authenticity of election outcomes***. This exemption, in conjunction with the lack of independent audits, reflects a ***systemic violation of federal standards, posing a serious risk to both Washington State and national election security.***

By restricting access to critical information, Washington's legislative policies have created an opaque election process that lacks public accountability, reinforcing a regulatory environment where non-compliance goes unchallenged.

Clear and Present Danger to Election Security and National Security

The current cyberattack on Washington's judicial systems provides a ***real-time demonstration of the security risks introduced by Washington's systemic cybersecurity failures.*** Without proper adherence to federal standards, Washington's election systems

remain ***highly vulnerable, posing an ongoing threat to public safety and election legitimacy:***

- **Immediate Risk of Lateral Movement**: Given the ***interconnected nature*** of Washington's critical infrastructure, attackers targeting one area, such as the judicial systems, ***can leverage these breaches to access related systems. CrowdStrike Falcon's limited endpoint detection capabilities and the vulnerabilities within its dependencies create ideal conditions for lateral attacks, placing election systems at immediate risk.***
- **Non-Certifiability of Election Results**: In light of the non-compliance with **EO 13800**, ongoing legislative concealment of key audit information, and the failure to meet federal cybersecurity standards, Washington's election process ***cannot be lawfully certified.*** **The systemic lack of compliance, transparency, and adherence to federal standards invalidates Washington's election certification claims, undermining public trust and eroding the foundation of lawful election processes.**
- **Broader National Security Threat**: Washington's ***failure to secure its election infrastructure*** has broader implications for **national security.** The reliance on vulnerable systems, combined with legislative exemptions from transparency, leaves the state's infrastructure ***exposed to manipulation by foreign actors.*** This creates a high-risk environment that can ***extend beyond Washington, compromising the national security of election systems across the U.S.***

Systemic National Security Threats from Washington's Cybersecurity Failures

Washington's disregard for federal cybersecurity standards and its failure to adhere to **EO 13800**, compounded by legislative policies that conceal essential audit information, have created a ***systemic risk to both state and national security.*** The reliance on **CrowdStrike Falcon**, with its known third-party vulnerabilities, and the lack of **Inspector General** oversight underscore a fundamental flaw in Washington's approach to election security.

The ongoing cyberattack affecting Washington's judicial systems further illustrates the **clear and present danger** posed by these vulnerabilities. Without a thorough course correction to ensure compliance with federal standards, transparency in audit information, and independent verification of security measures, Washington's election

infrastructure will ***continue to operate unlawfully, with compromised security and public trust.***
