

Smartmatic

December 22, 2024

Their Article:

Prebunking: A New Tool Against Election Disinformation



Ever since 'fake news' disrupted crucial votes such as Brexit and the 2020 US Presidential Election, election stakeholders have been grappling with the challenge of disinformation. In fact, the deterioration of information ecosystems has become so pervasive and ubiquitous that it's recognized as one of the biggest threats to election integrity by organizations like the [World Economic Forum](#) and the [Brennan Center for Justice](#).

Fortunately, a relatively new tool, known as prebunking, is showing promising results in the fight against disinformation and other forms of misinformation.

The concept of prebunking can be compared to vaccination in medicine, where the body is exposed to a weakened form of a pathogen to stimulate an immune response without causing illness. Similarly, prebunking presents pre-emptive counterarguments to false claims, thereby strengthening resilience against future misinformation. As in medicine, prevention is more impactful than cure. The goal is to equip audiences with the ability to identify and resist misinformation before it gains traction.

Leading prebunking researchers at companies like Google's [Jigsaw](#) and academic institutions like the [University of Cambridge](#) realized that misinformation 'has an Achilles heel'. That is, it frequently employs repetitive tactics and patterns. By recognizing these patterns historically, they can anticipate and counteract future misinformation through pre-bunking. These researchers are among the main proponents of prebunking.

IDEA International, an intergovernmental organization that supports sustainable democracy worldwide, analyzed disinformation in 53 countries across all continents between 2016 and 2021. Their study revealed that election-related disinformation is indeed repetitive. Specifically, 48% of disinformation targets the vote counting and voting processes, and nearly 50% of all attacks occur during the voting period of the cycle.

This article appeared in the Election Insight newsletter. [Subscribe for free today. Click here.](#)

Allegations that technology has been hacked by foreign actors, that servers are located abroad, or that technology vendors are owned by nefarious entities are recurring themes. These claims became even more prevalent following the disinformation campaigns surrounding the 2020 U.S. Presidential Election.

Given the repetitive nature of disinformation, election management bodies have an opportunity to anticipate where and how it will emerge. This foresight can be leveraged to design proactive strategies, or "vaccines," to combat disinformation effectively.

A key advantage of prebunking is its focus on addressing broader narratives and the underlying manipulation techniques used to spread misinformation. Unlike fact-checking or warning labels on social media, which concentrate on debunking individual claims, prebunking takes a wider view of the information ecosystem. This broader perspective allows election management bodies to tackle disinformation proactively, without appearing politicized in their responses to false claims. Moreover, by exposing the techniques behind disinformation rather than targeting specific content, prebunking reduces the risk of accusations of infringing on free speech, offering a balanced and effective approach to safeguarding public trust.

While prebunking in elections is relatively new, promising experiences in recent elections provide reasons for optimism. Researchers from [Yale University](#) and the [University of California, San Diego](#), demonstrated in a study that watching a prebunking video explaining the reasons behind the time taken to count ballots can significantly increase trust in election outcomes. This approach can mitigate up to 4 out of the 6 percentage points of distrust caused by reporting delays.

Although prebunking may not be a panacea, when it is well-implemented and combined with other techniques such as debunking, labeling, and voter literacy, it becomes an invaluable tool for election management bodies in the fight against disinformation.



11/19/2024 Uncategorized

Order

Our vision & mission

Our vision
The future of democracy is digital.

Our mission
Smartmatic's mission is to increase integrity in the democratic process.

We increase citizen engagement and trust, enabling better societies and better governments.

Smartmatic Case Studies

Los Angeles County - Voting Solutions for All People

Belgian elections 2012 - 2019 Customized voting solution for a pioneer in electronic voting.

Estonian elections 2014 - 2019 Solution for the world's leader in online voting.

Latest articles

Prebunking: A New Tool Against Election Disinformation

Election Trust Grows with Effective Public Communication

Eduardo Cornejo: "Modifying the AI Hype in Electoral Processes"

Stay updated



The Truth:

The article above from Smartmatic, while ostensibly discussing the solution to disinformation through prebunking, subtly employs several psychological manipulation tactics aimed at controlling the narrative and conditioning public perception:

Establishing Authority and Credibility: By citing what some people think are esteemed organizations like the World Economic Forum and the Brennan Center for Justice, Smartmatic attempts to position itself as some kind of authority on election integrity. This tactic leverages the halo effect, where the positive attributes of these respected institutions are transferred to Smartmatic, enhancing its perceived trustworthiness without necessarily proving its own systems' reliability.

Fear-Mongering: The article begins with a dire warning about the threat of disinformation to elections, invoking fear about the 'deterioration of information ecosystems'. This emotional manipulation tactic is designed to make readers anxious about the integrity of elections, thereby making them more receptive to Smartmatic's proposed solution, prebunking. Sadly, fear sells.

Repetitive Pattern Recognition: Smartmatic describes misinformation as having repetitive tactics, suggesting that they are well-versed in these patterns due to their research and partnerships with academic bodies like Cambridge and Google's Jigsaw. This establishes a narrative where Smartmatic is the expert in identifying and countering disinformation, subtly implying that their proprietary systems are above scrutiny because they understand the threats better than anyone else.

Prebunking as Conditioning: The concept of "prebunking" itself can be seen as a conditioning tactic. By framing prebunking as a

preventive measure against misinformation, Smartmatic is conditioning the public to accept their narrative before any counter-narrative can even be formed. This preemptive strategy is designed to inoculate the public against questioning Smartmatic's systems or practices, by preemptively discrediting potential criticisms as disinformation.

Generalization Over Specificity: By focusing on the broad techniques of disinformation rather than addressing specific instances or criticisms of their own systems, Smartmatic avoids detailed scrutiny. This tactic diverts attention from any potential flaws in their technology by generalizing the problem, making it seem as if any critique is just another example of the disinformation they are combating.

Appeal to Public Trust: The article suggests that prebunking combats disinformation without appearing politicized, thus positioning Smartmatic as an impartial guardian of the electoral process. This can be seen as an attempt to manipulate public trust by presenting themselves as defenders of democracy rather than as the commercial entity with vested interests that they are.

Selective Research Presentation: Mentioning specific studies that support prebunking while not addressing the potential for misuse or the criticisms of such methods is yet another form of manipulation. It presents a one-sided view that conveniently favors Smartmatic's narrative on election integrity.

Their intent here appears to be not to inform, but to preemptively shape public opinion in a way that discourages skepticism or new, potentially damaging, information about Smartmatic's voting systems. This article can be seen as an effort to condition citizens to trust Smartmatic's proprietary and opaque systems over public transparency and open scrutiny,

which are fundamental to democratic accountability.

I encourage all citizens NOT to fall for these tactics, and instead to question the motives behind such information operations. The only way for the people to legitimately trust THEIR elections is if the PEOPLE are who once again run THEIR elections. Remember, EARNED trust is worlds better than MANDATED trust, especially by those who profit on our blind trust.

Scott McMahan

December 22, 2024

PRIVATE PAGE – DO NOT SHARE!

A wonderful REAL journalist calls Scott out on a recorded phone call

2024-12-18 11th Hr Clements, Tore, Raiklin, Flynn and more CO Whistleblower w QA

Part 1

[Download Part 1 Transcript](#)

Part 2

[Download Part 2 Transcript](#)

Original Spaces Link:

<https://twitter.com/TishaLee777/status/1869555641733505463>

A fun chat with Grok about Dominion and Testing Labs

December 22, 2024

If the testing labs that tested Dominion's software missed the existence of SSMS and SQLCMD that allow modification of the

voting system database bypassing the application security controls, would you still categorize their testing as 'rigorous'?

If the testing labs missed the existence of SQL Server Management Studio (SSMS) and SQLCMD utilities, which could potentially allow for unauthorized modification of the voting system database by bypassing application-level security controls, then categorizing their testing as 'rigorous' would be problematic. Here's why:

Assessment of Rigor:

1. Scope of Testing:

- **Lack of Comprehensive Testing:** Rigorous testing should include an examination of all possible interfaces and access points to the database. Missing the presence or potential misuse of powerful database management tools like SSMS and SQLCMD indicates a significant oversight in the scope of security testing.

2. Security Controls:

- **Application vs. Database Security:** If these tools were present but not accounted for in the security architecture, it suggests that the testing did not adequately assess how database access was secured or how it could be exploited. Rigorous testing would involve ensuring that database access through any means, including direct SQL commands or management tools, adheres to the same security standards as the application.

3. Bypassing Controls:

- **Vulnerability to Bypass:** The ability to bypass application security controls through these utilities would be a major security flaw. A rigorous test would aim to identify such vulnerabilities, either through penetration testing, code review, or configuration checks.

4. Authentication and Authorization:

- **Failure in Access Management:** If SSMS and SQLCMD were accessible in a way that allowed unauthorized or improperly privileged access, this indicates a failure in authentication and authorization checks, which should be a key focus of any thorough security assessment.

5. Audit and Monitoring:

- **Lack of Detection:** Rigorous testing would also ensure that any use or attempted use of such tools would be logged, monitored, and alarmed, potentially preventing or at least detecting unauthorized access.

Implications:

- **Reassessment of Certification:** If such a significant oversight occurred, it would likely warrant a reassessment of the certification process for the voting systems. Election systems should be subjected to stringent security checks that account for all possible attack vectors, not just those within the application's direct control.
- **Trust and Integrity:** The integrity of the voting process relies heavily on trust in the systems used. Missing such

a critical aspect of system security could undermine public confidence in the voting machines' integrity.

▪ **Recommendations for Future Testing:**

- **Expanded Scope:** Future testing would need to explicitly include checks for database management tools and their potential misuse.
- **Enhanced Training:** Testers should be trained to think beyond the application layer, considering all possible avenues of database access.
- **Regular Audits:** More frequent and in-depth audits might be necessary, perhaps with a focus on both static and dynamic analysis of how databases are accessed and managed.

In conclusion, if the testing labs overlooked these tools, the term 'rigorous' would not appropriately describe their testing process. It would suggest a need for a more comprehensive approach to security testing, especially in environments where system integrity is paramount.

If a professional testing lab missed software that was on the 'Start Menu', what does that say about their attention to detail and expertise?

If a professional testing lab missed software that was accessible from the 'Start Menu', it would raise significant concerns about their attention to detail and expertise in several ways:

Attention to Detail:

- **Oversight:** The 'Start Menu' is one of the most visible and commonly used interfaces in Windows systems. Missing

software there suggests a lack of thoroughness in examining even the most obvious elements of the software environment. This oversight indicates that the lab's testing processes might not have included comprehensive checks of the user interface or might have been too focused on specific areas, neglecting the broader system overview.

- **Checklist and Procedure Failures:** Professional testing often involves checklists or systematic procedures to ensure all aspects of a system are examined. If software on the 'Start Menu' was missed, it could mean that these procedures are either not exhaustive or not followed meticulously.

Expertise:

- **Lack of Familiarity with OS:** Expertise in software testing includes a deep understanding of the operating systems and environments in which software operates. Missing something as fundamental as the 'Start Menu' might suggest that the testers are not sufficiently familiar with the operating system or did not apply their knowledge effectively in this context.
- **Security Implications:** For testing labs, particularly those dealing with sensitive applications like voting systems, security is paramount. Missing software on the 'Start Menu' could imply vulnerabilities in identifying all software that might interact with or affect the system under test, which is a critical aspect of security assessments.
- **Quality Control:** This oversight would question the quality control mechanisms in place at the lab. If such a basic element was missed, it might reflect on how other, potentially more complex or hidden issues might also be

overlooked.

Potential Reasons:

- **Scope Limitation:** Perhaps the testing was narrowly scoped to specific functionalities or modules, excluding a full system check, which would be a methodological flaw.
- **Time and Resource Constraints:** If testers were under pressure to meet deadlines or lacked resources, they might have cut corners or rushed through parts of the testing process.
- **Human Error:** Even with expertise, human error can occur, but frequent or significant oversights would indicate systemic problems in training or oversight.

Implications:

- **Credibility:** This incident would undoubtedly impact the credibility of the testing lab. Clients expect professional labs to have the expertise and diligence to catch even what might seem like minor details, as these can have significant implications in software functionality or security.
- **Need for Review:** It would necessitate a review of their testing methodologies, possibly involving retraining, revising testing protocols, or integrating new tools or checklist items to ensure no aspect of the software environment is overlooked.
- **Public and Client Trust:** In fields like election software testing, where public trust is crucial, such an oversight could lead to skepticism about the integrity of the testing process, potentially affecting future contracts or certifications.

In summary, missing software on the 'Start Menu' in a professional testing context would suggest that there are gaps in the lab's attention to detail and possibly in their expertise application. It would prompt a reevaluation of their testing practices to ensure they meet the high standards expected in professional software testing.

For a testing lab that is testing software that was deemed part of our national critical infrastructure, to miss such obvious things, should this testing lab be trusted at all at this point?

If a testing lab responsible for evaluating software critical to national infrastructure missed something as ostensibly straightforward as software listed on the 'Start Menu', it raises serious concerns about their reliability and competence. Here are several points to consider:

Trust Implications:

1. Compromised Integrity:

- **Missed Vulnerabilities:** If basic elements are overlooked, there's a high likelihood that more complex or hidden vulnerabilities might also be missed. This is particularly alarming for national critical infrastructure where the consequences of failure can be catastrophic.

2. Lack of Thoroughness:

- **Systematic Oversights:** This incident suggests that the lab's testing methodologies might be flawed or not comprehensive enough. For critical infrastructure, testing needs to be exhaustive, leaving no stone unturned.

3. Expertise and Capability:

- **Professional Competence:** Such an oversight questions the expertise of the testers or the lab's overall capability to handle sensitive and high-stakes testing. Trust in their technical ability to safeguard national interests would be notably diminished.

4. Security and Safety Concerns:

- **National Security:** Missing software on the 'Start Menu' could imply that the lab might not have the necessary depth in security testing, potentially leaving the nation's infrastructure exposed to cyber threats or operational failures.

5. Public Confidence:

- **Trust Erosion:** Public trust in the security and reliability of critical infrastructure relies on confidence in the systems that protect it. An oversight like this could erode that trust, particularly if it becomes public knowledge.

Actions to Consider:

- **Immediate Review:** There should be an immediate and thorough review of all testing conducted by the lab, especially for critical infrastructure systems. This might involve third-party re-audits or re-testing by another lab.
- **Process Improvement:** The lab should revise its testing methodologies, possibly adopting more rigorous or automated checks, enhancing training, and ensuring that

all aspects of the system are tested, including the most apparent interfaces like the 'Start Menu'.

- **Transparency:** The lab should be transparent about this incident, detailing how it occurred, what steps are being taken to rectify the issue, and how they will prevent such oversights in the future.
- **Accountability:** There might need to be accountability measures for those responsible for the oversight, potentially including retraining or reassessment of staff, or even contractual repercussions if the lab's services were under government or critical infrastructure contracts.
- **Certification and Accreditation:** Reevaluation of the lab's certifications or accreditations might be necessary, especially if these are tied to the ability to test critical infrastructure software.

Conclusion:

At this point, the trust in this testing lab would be seriously compromised unless they can demonstrate a strong corrective action plan and show that this was an isolated incident due to exceptional circumstances rather than indicative of systemic issues. For national critical infrastructure, where the margin for error is extremely low, any lab with such an oversight would need to prove its reliability through actions, not just assurances. If confidence cannot be restored, it might be prudent for stakeholders to consider alternative testing entities until trust is reestablished.

If the installation program of the Dominion EMS server opened firewall ports and allowed connections from all ip addresses instead of limiting those connections to particular subnets or specific IP addresses, in a system that is deemed CRITICAL INFRASTRUCTURE, could that be considered criminal negligence of

the highest degree?

If the installation program for the Dominion Election Management System (EMS) server indeed opened firewall ports allowing connections from all IP addresses without any restrictions, in a system classified as critical infrastructure, this could potentially be considered criminal negligence, depending on several factors:

Analysis:

1. Security Implications:

- **Open Ports to All IP:** Allowing connections from all IP addresses would expose the system to a vast array of potential threats including unauthorized access, cyber-attacks, and data breaches. For critical infrastructure, this is highly risky as it increases vulnerability to cyber threats exponentially.

2. Industry Standards and Best Practices:

- **Security Protocols:** Best practices in cybersecurity, especially for critical infrastructure, dictate that access should be restricted to specific, trusted IP addresses or subnets, following the principle of least privilege. Opening ports to all IP addresses would violate these standards, suggesting a significant lapse in security configuration.

3. Legal and Regulatory Framework:

- **Criminal Negligence:** For an act or omission to be considered criminal negligence, it must show a gross deviation from the standard of care that a reasonable person would exercise in similar circumstances. Here, the act of leaving critical

infrastructure open to the entire internet could be seen as such a deviation, especially if:

- There was knowledge or should have been knowledge of the risks involved.
- No reasonable steps were taken to prevent such risks.

4. Intent and Awareness:

- **Negligence vs. Intent:** Criminal negligence would not require intent but would hinge on the foreseeability of harm and the failure to act to prevent it. If the developers or installers were aware or should have been aware of the security implications and failed to address them, this could constitute negligence.

5. Impact on Critical Infrastructure:

- **Potential for Harm:** Given the nature of election systems as critical infrastructure, where security failures could affect national elections, public trust, and democracy itself, the potential for harm is immense. This context elevates the severity of any security oversight.

6. Response and Mitigation:

- **Post-Install Actions:** If there was an immediate and effective response to rectify this issue after it was discovered, the perception of negligence might be mitigated. However, the initial setup and lack of default security measures would still be highly criticized.

Legal Considerations:

- **Laws and Regulations:** Specific laws like the Computer Fraud and Abuse Act in the U.S., along with regulations from bodies like the Election Assistance Commission (EAC), set standards for electronic voting systems. Violating these by exposing systems to undue risk could potentially lead to legal repercussions, including criminal charges if negligence is proven.
- **Jurisdiction:** The legal implications could vary by jurisdiction, depending on local laws regarding cybersecurity, critical infrastructure protection, and election integrity.

Conclusion:

While opening all firewall ports to all IP addresses in such a critical system would certainly be seen as gross negligence from a cybersecurity perspective, whether it constitutes “criminal negligence of the highest degree” would depend on legal interpretation, the specifics of how this occurred, and the response to the issue. It would likely be subject to a thorough investigation by legal, cybersecurity, and possibly election oversight bodies to determine if criminal negligence had taken place, considering both the intent and the impact on national security and electoral integrity.

If a testing lab, tasked with the job of testing critical infrastructure such as this were to also miss this, would their credibility suffer another extreme blow?

If a testing lab, already tasked with evaluating software for critical infrastructure like the Dominion EMS server, missed an issue where the installation program leaves firewall ports open to all IP addresses, their credibility would indeed suffer

another extreme blow for several reasons:

Reasons for Credibility Loss:

1. **Previous Oversights:** If this incident follows any previous mistakes or oversights, especially those involving basic security configurations, it would compound doubts about the lab's competence and reliability. Each new oversight adds to a pattern of negligence or incompetence.
2. **Critical Nature of the Infrastructure:** The importance of securing critical infrastructure cannot be overstated. Missing a fundamental security flaw like open firewall ports indicates a failure to appreciate or address the severity of risks involved, which is contrary to the expectations set for testing such systems.
3. **Scope of Testing:** This kind of oversight suggests that the lab might not be testing with the appropriate scope or depth, potentially focusing on functionality at the expense of security, which is a critical aspect of testing for infrastructure deemed vital to national interest.
4. **Public and Stakeholder Trust:** The public and stakeholders, including government bodies, rely heavily on the assurance that systems critical to democracy and national security are thoroughly vetted. Each missed vulnerability erodes this trust, especially in an era where cybersecurity threats are a top concern.
5. **Professional Standards:** The lab's adherence to professional standards, best practices in cybersecurity, and specific guidelines for testing election systems would come into question. This could lead to repercussions like loss of certifications, legal challenges, or exclusion from future critical infrastructure projects.
6. **Reputational Damage:** Beyond immediate professional consequences, the reputational damage could be long-

lasting. Other clients might reconsider their association with the lab, fearing similar oversights in their projects.

Potential Consequences:

- **Review and Audit:** There would likely be an immediate call for an independent review or audit of all testing conducted by the lab, not just for Dominion's systems but potentially for all critical infrastructure projects they've worked on.
- **Reevaluation of Processes:** The lab would need to reassess its testing methodologies, possibly overhaul its approach to security testing, and might need to invest in better tools or training.
- **Legal and Regulatory Scrutiny:** There could be legal implications if the oversight leads to breaches or if it's found that the lab did not comply with mandatory testing protocols. Regulatory bodies might investigate or impose sanctions.
- **Transparency:** The lab would need to be transparent about how such an oversight occurred and what measures are being taken to prevent future occurrences. This might involve public or client apologies, detailed reports, or public demonstrations of new protocols.
- **Loss of Business:** The lab could lose current and future contracts, particularly those involving national security or critical infrastructure, as clients seek more reliable testing partners.

Conclusion:

Missing something as fundamental as open firewall ports in critical infrastructure testing would severely undermine the

lab's credibility. It would not only reflect poorly on their technical capabilities but also on their understanding of the implications of such vulnerabilities in systems vital to national security. This incident would likely be the catalyst for significant changes within the lab or even its replacement by competitors with a stronger track record.

Even if the vendor tries to claim that it isn't a problem because these systems are 'not supposed to be on the internet', what are the potential issues considering this is a system deemed as critical infrastructure?

Even if a vendor claims that these systems are "not supposed to be on the internet," there are still significant potential issues with critical infrastructure like election management systems (EMS) that open firewall ports to all IP addresses:

Potential Issues:

1. Physical Security Breaches:

- **Local Network Access:** While the system might not be directly connected to the internet, if it's accessible via any network (even an isolated one within a facility), an attacker with physical access could still exploit this vulnerability. Physical security breaches can lead to network access.

2. Misconfiguration or Human Error:

- **Unintended Connectivity:** Systems might inadvertently connect to broader networks or the internet due to misconfiguration, human error, or through the use of other networked devices (like printers or USB drives with network capabilities). This could expose the system to external threats.

3. **Social Engineering and Insider Threats:**

- **Internal Threats:** Employees or insiders might be tricked or coerced into connecting the system to the internet or another network, either intentionally or accidentally, thus exposing it. The open ports would then become a significant vulnerability.

4. **Network Segmentation Issues:**

- **Compromise of Adjacent Systems:** If the EMS is on a network with other systems that do have internet access, a breach in one system could lead to lateral movement by attackers into the supposedly isolated EMS.

5. **Legacy Systems or Updates:**

- **Integration with Other Systems:** Election systems often need to integrate with other systems for data transfer, updates, or maintenance. If these connections are not managed securely, they could provide a pathway for external access.

6. **Future Connectivity Needs:**

- **Scalability and Maintenance:** There might be future needs or upgrades where internet connectivity becomes necessary for software updates, remote diagnostics, or other purposes. If the system is already configured to accept connections from any IP, this could be exploited before proper security measures are implemented.

7. **Testing and Development Environments:**

- **Development Leaks:** Systems might be tested or developed in environments that do have internet

access. If these configurations carry over to production without proper review, the vulnerability persists.

8. **Third-Party Services or Vendors:**

- **Vendor Access:** Sometimes, vendors or third-party services need remote access for support or maintenance. If this is not tightly controlled and the system is set to accept connections from any IP, unauthorized access could occur.

9. **Emergency Situations:**

- **Crisis Management:** In emergencies, there might be a rush to connect systems to get quick access to data or to manage the situation, potentially bypassing established security protocols.

10. **Regulatory and Compliance Failures:**

- **Audit and Compliance:** Even if not connected to the internet, having such a configuration could fail audits or compliance checks, leading to legal, financial, or reputational damage.

Implications for Critical Infrastructure:

- **Risk to Democracy:** Election systems are pivotal to democratic processes. Any security lapse could undermine public trust, potentially affecting election outcomes or perceptions thereof.
- **National Security:** Compromise of such systems could lead to broader national security implications, affecting not

just elections but potentially other systems if attackers gain a foothold.

- **Cascading Effects:** Critical infrastructure often has interdependencies. A breach in one area could have cascading effects, impacting other sectors or services.
- **Reputation and Trust:** The credibility of the vendor, the testing labs, and the electoral process itself would be at stake, leading to potential long-term damage to public confidence.

In conclusion, even with claims of isolation from the internet, the configuration of open ports to all IP addresses in critical infrastructure like an EMS represents a severe security flaw with numerous potential vectors for exploitation. It's a scenario that necessitates immediate remediation and would likely prompt a significant overhaul of security practices and policies.

If a vendor created software with even these few issues and they knew their software was deemed part of critical infrastructure, what type of severity would this violation be?

Given that the software in question is part of critical infrastructure, particularly in the context of election management systems, the severity of the issues described would be categorized as follows:

Severity Classification:

1. Critical Severity:

- **Open Firewall Ports to All IPs:** This issue is of **critical severity** because:
 - **Impact:** It directly affects the confidentiality, integrity, and availability of the system. Any unauthorized access could

lead to data manipulation, system compromise, or disruption of election processes.

- **Exposure:** By allowing connections from all IP addresses, the system is exposed to every potential attacker on the internet or within any network it might be connected to, even unintentionally.
- **Risk to Critical Functions:** For a system integral to democracy, where security is paramount, this vulnerability could lead to catastrophic outcomes, including election tampering, which undermines national security and public trust.

2. High Severity:

- **Misconfiguration or Human Error Leading to Internet Exposure:** Assuming this is a known risk or has been observed in practice, this would be considered **high severity** because:
 - **Potential Impact:** While not immediately exploitable without further action (like connecting to the internet), the configuration leaves the system open to such risks if any part of the network becomes internet-facing.
 - **Systemic Vulnerability:** It indicates a systemic issue in the software's default setup or documentation, showing a lack of understanding or concern for the security requirements of critical infrastructure.

3. High Severity:

- **Lack of Proper Network Segmentation or Security Controls:** If the software does not enforce or guide users towards proper network isolation or segmentation, this is also **high severity** due to:
 - **Indirect Exposure:** Even without direct internet access, poor network segmentation could allow an attacker to move laterally from another compromised system to the EMS.

Justification for Severity:

- **Critical Infrastructure Standards:** Any software used in critical infrastructure should adhere to the highest security standards. The presence of such vulnerabilities directly contradicts the security expectations for systems like EMS, which are under intense scrutiny for integrity and reliability.
- **Regulatory and Compliance Perspective:** From a compliance standpoint, these issues would violate numerous security standards and regulations designed to protect critical infrastructure, potentially leading to legal and financial repercussions for the vendor.
- **Public Confidence and National Security:** The implications for public trust and national security are profound. Even the perception of vulnerability in electoral systems could have far-reaching consequences.
- **Vendor Responsibility:** If the vendor knew or should have known that their software was to be used in critical infrastructure, the failure to address these basic security measures could be seen as gross negligence or, in a legal context, potentially criminal negligence, given

the foreseeability of harm.

Conclusion:

These issues, particularly in the context of critical infrastructure like election systems, would be classified as critical or high severity vulnerabilities. They demand immediate attention, remediation, and potentially a complete overhaul of the software's security architecture. The vendor would likely face severe scrutiny, potential litigation, and a significant reputational hit if these issues were exposed or exploited.

and what violations would there be for the testing lab?

If a testing lab, responsible for evaluating software for use in critical infrastructure, missed these severe security issues, they could potentially be held accountable for several types of violations or failures:

Violations and Failures:

1. Failure to Comply with Testing Standards:

- **Non-adherence to Protocols:** Labs are often required to follow specific protocols and standards for testing, especially for critical infrastructure. Missing critical vulnerabilities like open firewall ports would indicate a failure to meet these standards, potentially violating agreements or certifications with bodies like the Election Assistance Commission (EAC) or the National Institute of Standards and Technology (NIST).

2. Negligence in Security Assessment:

- **Security Oversight:** If the lab did not include or adequately perform security testing that would have

revealed these vulnerabilities, this could be seen as professional negligence. This is particularly severe when dealing with systems that manage national elections.

3. Breach of Contract:

- **Contractual Obligations:** Testing labs typically have contractual obligations to thoroughly test and verify the security of software. Failing to identify such basic yet critical flaws could lead to breach of contract claims from clients or the government.

4. Regulatory Non-Compliance:

- **Regulatory Violations:** Depending on the jurisdiction, there might be specific regulations regarding the testing of software for critical infrastructure. Missing these vulnerabilities could lead to violations of laws or regulations aimed at protecting national security, data integrity, or election processes.

5. Professional Ethics and Standards:

- **Ethical Violations:** Professional bodies might view such an oversight as a violation of ethical standards or professional conduct, potentially leading to sanctions, loss of accreditation, or professional membership.

6. Loss of Certification:

- **Certification Revocation:** If the lab holds certifications from bodies like ISO/IEC 17025 (for testing and calibration labs), missing critical security flaws might lead to an investigation and

possibly the revocation or suspension of these certifications.

7. **Public Trust and Accountability:**

- **Public Accountability:** There could be public or governmental inquiries, especially in the context of elections, leading to accountability measures or even legal action if public trust is significantly undermined.

8. **Financial Liability:**

- **Damages:** If the missed vulnerabilities lead to actual harm or breaches, the lab could be financially liable for damages, especially if it can be proven that their negligence directly contributed to the security failure.

Specific Violations:

- **Failure to Identify Known Vulnerabilities:** Not detecting something as basic as open ports to all IPs is a clear failure to identify known security risks.
- **Inadequate Security Testing Scope:** The lab might have focused too narrowly on functionality or performance, neglecting comprehensive security assessments.
- **Lack of Rigorous Penetration Testing:** If penetration testing was part of their remit, not simulating attacks that would easily reveal such vulnerabilities is a significant oversight.
- **Poor Documentation and Reporting:** If the lab did not document or report on security configurations adequately, this would be another violation of expected testing

practices.

Conclusion:

The severity of these violations would depend on the specifics of their contract, the regulatory environment, and the actual impact of their oversight. However, the lab's credibility would be severely compromised, potentially leading to legal, financial, and reputational consequences. They would need to undertake significant steps to restore trust, including revising testing methodologies, retraining staff, and possibly facing external audits or certifications to re-establish their competence in testing critical infrastructure software.

and what violations would there be for election officials that were put on notice that some or all of these issues existed, yet still conducted the 2024 election using these systems?

Election officials who were aware of these critical security issues in election management systems (EMS) but chose to proceed with the 2024 election using them could potentially face a range of violations, depending on jurisdiction, specific laws, and the context of their decisions:

Potential Violations:

1. Breach of Election Integrity Laws:

- **Legal Requirements for Election Security:** Many jurisdictions have laws or regulations stipulating that elections must be conducted securely to ensure the integrity of the vote. Using known vulnerable systems could be seen as a direct violation of these laws.

2. Negligence or Gross Negligence:

- **Duty of Care:** Election officials have a duty to ensure the integrity of the electoral process. Knowing about critical vulnerabilities yet proceeding without remediation could be construed as negligence, especially if any harm or doubt about the election's integrity results.

3. Misuse of Public Office or Misconduct:

- **Public Trust:** Holding public office implies a responsibility to act in the public's interest. Using compromised systems could be seen as misconduct or an abuse of power, particularly if it leads to or could lead to the manipulation of election results.

4. Violation of Election Administration Regulations:

- **Certification and Compliance:** Election systems often need certification or must comply with certain standards. Deploying systems with known vulnerabilities could violate these certifications or compliance requirements.

5. Criminal Liability:

- **Criminal Negligence:** In extreme cases, where there's evidence that officials knew of the risks and ignored them, leading to significant harm (like affecting election outcomes), they could face criminal charges for negligence or endangerment.

6. Civil Liabilities:

- **Lawsuits:** Candidates, voters, or advocacy groups could sue election officials for negligence or malfeasance if they can prove that the use of

insecure systems compromised the election or their rights.

7. Violations of State or Federal Election Laws:

- **Specific Legislation:** There might be state or federal laws that explicitly require secure voting systems. Using known insecure systems could be a direct violation, potentially leading to both civil and criminal penalties.

8. Ethical Violations:

- **Professional Ethics:** Election officials are expected to adhere to high ethical standards. Proceeding with elections using systems known to have security flaws might be considered an ethical violation by oversight bodies or professional associations.

9. Failure to Protect Voter Data:

- **Data Protection Laws:** If the vulnerabilities involve the risk of voter data exposure, officials could be in violation of data protection regulations, which are increasingly stringent regarding personal information.

10. Non-Compliance with Cybersecurity Directives:

- **Federal or State Directives:** There might be specific cybersecurity directives from bodies like CISA (Cybersecurity and Infrastructure Security Agency) or state equivalents that election officials must follow. Ignoring these could lead to legal repercussions.

Considerations:

- **Public and Legal Scrutiny:** The decision to use insecure systems could lead to significant public outcry, legal challenges, and investigations, especially if there's any indication of election interference or fraud.
- **Post-Election Audits:** If issues are found post-election, officials might face scrutiny not only for the decision to use the systems but also for how they managed or reported on these issues.
- **Intent and Knowledge:** The severity of any potential violation would hinge on what officials knew, when they knew it, and their intent or negligence in proceeding with the election.

Conclusion:

Election officials using known insecure systems for an election could face a combination of civil, criminal, and administrative violations, depending on the specifics of the case. The public and legal consequences could be severe, potentially leading to the invalidation of election results, personal liability, and a significant loss of public trust in the electoral process.

what are the potential and minimum and maximum legal consequences for each entity involved?

Here are the potential legal consequences for each entity involved in using or failing to secure election management systems (EMS) for the 2024 election, categorized by minimum and maximum scenarios. Note that these are general possibilities and would vary based on jurisdiction, specific laws, and the details of each case:

Vendor (Software Developer):

Minimum Consequences:

- **Civil Penalties:** Fines for breach of contract or non-compliance with industry standards.
- **Reputational Damage:** Could lose business or see a decline in trust from clients.

Maximum Consequences:

- **Criminal Charges:** Potentially for gross negligence, fraud, or conspiracy if there's evidence of intentional wrongdoing or negligence leading to election tampering.
- **Significant Fines:** If found guilty under laws protecting critical infrastructure or election integrity, fines could be substantial.
- **Imprisonment:** For individuals directly involved, if criminal negligence or fraud is proven.
- **Business Closure or Restructuring:** Regulatory bodies might force the company to cease operations, restructure, or undergo severe oversight.

Testing Lab:

Minimum Consequences:

- **Loss of Certification:** Could lose accreditations necessary for operating as a testing lab.
- **Civil Claims:** Lawsuits from clients or affected parties for negligence leading to financial losses or compromised elections.

Maximum Consequences:

- **Criminal Liability:** If negligence leads to significant harm or if there's evidence of collusion or deliberate oversight, individuals could face criminal charges.
- **Large Fines:** For violating laws related to the security of critical infrastructure.
- **Professional Sanctions:** Loss of licenses or bans from professional bodies.
- **Business Dissolution:** In extreme cases, the lab might be forced to close if trust is completely eroded, or if regulatory action deems them unfit to continue.

Election Officials:

Minimum Consequences:

- **Administrative Penalties:** Could include reprimands, mandatory training, or restrictions on future responsibilities.
- **Civil Lawsuits:** From candidates or voters if the integrity of the election is questioned but without proving direct harm.

Maximum Consequences:

- **Criminal Charges:** For gross negligence, misconduct, or malfeasance if it's proven that officials knew of vulnerabilities and proceeded recklessly, potentially leading to election fraud.
- **Imprisonment:** If criminal charges stick, particularly in cases of intentional wrongdoing or severe negligence affecting election outcomes.
- **Election Nullification:** In extreme cases, if the integrity of the election is sufficiently compromised, courts might order re-elections or invalidate results.

- **Career Termination:** Loss of position, eligibility to hold future office, or professional licenses, depending on the severity of the violation and public outcry.

Additional Notes:

- **Civil Lawsuits:** Across all entities, civil lawsuits could seek damages for any harm caused by insecure systems, including reimbursement for costs associated with re-elections or security enhancements, and compensation for affected parties.
- **Regulatory Actions:** Governmental bodies might conduct investigations, leading to new regulations, oversight, or mandatory security protocols for future elections.
- **Public Trust:** The least quantifiable but most impactful consequence might be the loss of public confidence, which could lead to long-term political and social ramifications.
- **Jurisdictional Variance:** These consequences can vary widely depending on state or federal laws, the specifics of the incident, and the political climate. Some states might have more stringent election security laws, while others might not.
- **Intent vs. Negligence:** The legal outcomes would also hinge on whether actions or inactions were intentional or due to negligence, with intentional acts typically leading to more severe penalties.

In summary, while the minimum consequences might involve fines, reputational damage, or administrative penalties, the maximum could involve criminal charges, significant financial penalties, and career or business-ending repercussions.

And now answer the same but for criminal penalties.

Here are the potential criminal penalties for each entity involved in the scenario where they knowingly used or allowed the use of insecure election management systems (EMS) for the 2024 election:

Vendor (Software Developer):

Minimum Criminal Penalties:

- **Misdemeanor Charges:** For lesser offenses like failure to comply with mandatory security standards, potential fines, or up to one year in jail.

Maximum Criminal Penalties:

- **Felony Charges:**

- **Criminal Negligence:** If negligence results in significant harm or potential for harm to the election process, could face felony charges with penalties including:
 - **Fines:** Substantial monetary penalties, potentially in the hundreds of thousands or millions.
 - **Imprisonment:** Depending on jurisdiction, could range from 1 to 20 years or more if charged with crimes like fraud, conspiracy, or tampering with elections.
- **Fraud or Conspiracy:** If there's evidence of deliberate actions to mislead or manipulate elections, penalties could include:
 - **Longer Prison Sentences:** Potentially up to life imprisonment, especially in cases linked to national security threats.

- **Asset Forfeiture:** Seizure of company assets or personal assets of key figures involved.

Testing Lab:

Minimum Criminal Penalties:

- **Misdemeanor:** For negligence in testing procedures leading to minor breaches or oversights, fines or short jail terms.

Maximum Criminal Penalties:

▪ **Felony Charges:**

- **Gross Negligence:** If their failure directly or indirectly results in election compromise:
 - **Fines:** Significant fines, possibly in proportion to the impact on the election.
 - **Jail Time:** 1 to 10 years or more, depending on the perceived damage and legal jurisdiction.
- **Criminal Misconduct:** For knowingly falsifying or omitting critical security information:
 - **Prison Terms:** Could extend to 15 years or more for charges like perjury, fraud, or conspiracy in the context of national elections.
 - **Professional Consequences:** Loss of professional licenses or certifications, leading to career termination.

Election Officials:

Minimum Criminal Penalties:

- **Misdemeanor Charges:** For minor breaches of duty, like negligence in oversight, could face fines or up to one year in jail.

Maximum Criminal Penalties:

▪ **Felony Charges:**

- **Criminal Negligence or Malfeasance:** If officials were aware of the risks and still proceeded:
 - **Imprisonment:** Depending on the state, could range from 2 to 20 years or more, with cases of election tampering or gross negligence potentially leading to longer sentences.
 - **Fines:** Heavy fines to reflect the gravity of compromising an election.
- **Conspiracy or Fraud:** If there's evidence of deliberate intent to manipulate or jeopardize the election:
 - **Severe Prison Sentences:** Could extend to life imprisonment in extreme cases where national security or democratic integrity is at stake.
 - **Disqualification:** Barred from holding public office or similar positions in the future.

Additional Considerations:

- **Prosecution Variability:** The actual charges and penalties would depend on the specifics of the case, the strength of the evidence, and how laws in different jurisdictions interpret actions related to election security.
- **Intent vs. Negligence:** Intentional acts to compromise election security would likely lead to harsher penalties than negligence, though both can result in significant criminal consequences.
- **Aggravating Factors:** Factors like the scale of the election, the number of voters affected, or if there was a cover-up could escalate the severity of penalties.
- **Federal vs. State:** Federal charges could be brought if there's an interstate element or if federal election laws are violated, potentially leading to even more severe penalties.

In summary, criminal penalties could range from misdemeanor charges with fines and short jail time to felony convictions with substantial prison sentences and fines, especially if the actions are seen to undermine the democratic process or national security.

Mesa County Reports

December 22, 2024

[Report 1](#)

Work done by Mark Cook and Doug Gould:

[Report 2](#)

Work done by Mark Cook and Doug Gould:

[Report 3](#)

Work done by Jeff O'Donnell and Dr. Walter Daugherty:

**All these reports are also available on TinaPeters.us. Please go to this site and help Tina, who has stood up for all not only Coloradans, but also All Americans!*

Progressive Election Platform

December 22, 2024

[Click here to see the Proposed Executive Order to get the party started!](#)

Scope

At the heart of democratic governance lies the voting system, a mechanism designed to reflect the collective will of the people. For this system to truly serve its purpose, it must be **so simple and transparent** that **every citizen**, regardless of their background, education, or technological literacy, can not only participate but also **understand and verify every step** of the process. This simplicity and transparency are not just about ease of use; they are fundamental to **ensuring equal access** to the electoral process. If the mechanics of voting are shrouded in complexity or lack transparency, trust in the electoral outcome diminishes, eroding the foundation of our republic. At its essence, voting involves eligible citizens marking their choices on paper, followed by a straightforward count of these marks. This process doesn't necessitate elaborate or costly technology; instead, it demands clarity, accessibility, and the ability for public oversight. For American citizens to genuinely reclaim their electoral process, immediate and comprehensive reforms are imperative. Here's what we must implement:

Voter Registration

- Counties must once again become the SOLE CUSTODIAN of their County Voter Registrations.
- Counties must be the SOLE ARBITER of registrant eligibility.
- Every 2 years (4 at the most, as longer leads to less accurate information)
- In-person at the county
- Verified citizen and residency check at that time
- Paper voter registration cards (this is a great place to

ask for election volunteers!)

- Witnessed signature
- Stored by voting precinct
- A read-only standardized (UNIVERSAL FORMAT) digital list of registered voters is provided by every county on their website to share with the citizens and all other counties.
- Each county cross-references their list against all other counties. Paper poll books for each precinct are created from registration cards prior to every election.
- A national unique voter number assigned to each voter would greatly improve registration integrity.

Absentee Ballots

- Limited to as-needed basis
- Proof must be provided and accepted
- Extreme scrutiny must be placed on every incoming ballot, with additional integrity mechanisms
 - OPTIONAL IMPROVEMENT: A Ballot choice 'hash' (digital 'fingerprint' of the voted ballot choices – not an actual fingerprint from a finger) could be developed that could be used as additional form of received ballot integrity
- Military Absentee ballots must be identified as such. Non-Military Absentee ballots must be identified , and both should also look different than in-person ballots to ensure they all remain discrete.
- **There is no way to absolutely guarantee that the ballot received and tabulated is the same ballot that was sent by the voter, without violating ballot secrecy. This is why Absentee voting is so vulnerable.*

Election Day

- One day voting holiday
- Elections at the precinct (each precinct \leq 1500 population)
- *An idea to further minimize engineered manipulation: Standardized FIXED voting start/end/duration across the country to eliminate time-staggered abuse vector (14-hour voting period, for example) – This will require some work and thought!*
 - West coast would be starting at 5a and ending at 7p
 - East coast voting would start at 9a and end at 11p
 - 100% registered and participated, would result in just under 2 voters per minute max needed throughput. If each voter takes 6 minutes to fill out the ballot, one would need to have minimum 6 voting booths per precinct. If people arrive with cheat sheets, this is all easily doable.
- Checked in on paper poll book
- Witnessed signature
- Cross-referenced with previously filled out voter registration card
- No early or late ballots
- Paper ballots dropped in translucent locked container
- Entire room on video

Election Night

- No ballots accepted after poll close.
- At poll close, all ballots:

- Separated by Military Absentee, Non-Military Absentee, In-person.
 - Batched (pick up 25 ballots then randomize in order for ballot secrecy).
 - Scan the batch to produce digital images in a PDF.
 - Votes COUNTED WHERE CAST
 - Under High Definition video
 - Bi-partisan citizens and witnesses using state-approved hand tabulation method
- Results released right then by precinct and posted on the outside of the building for all to see/verify

Reporting

- Each precinct posts the signed precinct results on the outside of the building, the same page that was scanned during tabulation.
- All ballot images, tally sheets, results pages, other paperwork, and video put on county website grouped by precinct for anyone and everyone to verify all they like.
 - Just like I did here: <https://openelectionrecords.org/ar-searcy-county-2024-03-05/>
- Discrete reporting by voting type: Military Absentee, Non-Military Absentee, In-person.
- Our election officials should be **Election Transparency Agents**, who's duties are ensuring that all chain of custody and election records are both preserved and both

made public to enable exhaustive audits to be performed by any American Citizen that desires to do so.

Auditing

- Students in 6-12th grades
 - Civics refresher
 - Election refresher
 - Break into groups
 - Pull up their school's precinct ballots from county website
 - Students re-tabulate the ballots themselves
 - Compare results
 - If there is any discrepancy
 - Students submit through a standardized reporting form on County Website
 - County celebrates the catch and publicly awards the class

- Advanced math students could then dive into the statistics of the elections to identify inorganic patterns

- Public
 - The public can access all election data on the county website and audit to their hearts content
 - Voted lists
 - Ballot tabulation
 - Chain of Custody
 - Statistics

THE ABOVE IS A WORK-IN-PROGRESS. If you have suggestions, please reach out!

You can find me on X @PatriotMarkCook

Election Day Notice for Election Departments

December 22, 2024

THE FOLLOWING IS JUST A SAMPLE AND IS NOT LEGAL ADVICE

[Your Name]

[Your Address]

[City, State, Zip Code]

[Email Address]

[Phone Number]

[Date]

To: [Election Official's Name]

From: [Your Name/Office]

Date: [Current Date]

Subject: Urgent Election Day Preparations – Legal Obligations, Backup Plans, Transparency, and Observers

Dear [Election Official],

Given the projected unprecedented voter turnout for this pivotal

election, and the critical role this election plays in our democracy, you are hereby notified of your legal obligations under federal and state election laws. This notice serves to emphasize the importance of your preparation to accommodate a potentially record-breaking number of voters while ensuring compliance with the Help America Vote Act (HAVA), the Americans with Disabilities Act (ADA), and the Voting Rights Act of 1965.

Legal Responsibilities:

1. Compliance with the Help America Vote Act (HAVA):

- **Section 301:** Ensure voting systems provide for accessible voting for individuals with disabilities.
- **Section 905:** Outlines penalties for conspiracy to deprive voters of a fair election or providing false information in registering and voting.

2. Americans with Disabilities Act (ADA):

- Polling places must be physically accessible, and voting processes must accommodate those with disabilities.

3. Voting Rights Act of 1965:

- Prohibits practices that could result in discriminatory effects, including unnecessarily long waits that might disproportionately affect certain groups.

Preparation Steps:

1. Increase Polling Locations:

- Ensure compliance with state laws on polling place

distribution.

2. Staffing and Training:

- Train staff in both electronic and manual voter processing techniques.

3. Voting Equipment:

- Ensure all voting machines are tested and functional, with backups.

4. Dual Check-In Systems:

- **Primary Electronic Check-In:** Utilize technology for efficiency.
- **Manual Paper-Based Backup:**
 - **Preparation:** Keep updated paper voter rolls and emergency ballots.
 - **Implementation:** Train staff to switch to manual methods swiftly.

5. Transparency and Chain of Custody for Manual Processes:

- **Chain of Custody:**
 - Document every step of manual ballot handling, from receipt to deposit.
 - Securely seal ballot boxes, with records of who seals them.
- **Transparency Measures:**
 - Ensure poll watchers and observers have clear visibility of all processes, except where voter privacy is concerned.
 - Maintain detailed logs of manual operations

for audit purposes.

6. Voter Education:

- Communicate potential use of manual systems to voters.

7. Weather Considerations:

- Provide adequate protection for voters in extreme weather.

8. Accessibility:

- Ensure accommodations for disabled and elderly voters.

9. Voter Assistance:

- Prepare for alternative voting methods like curbside voting.

10. Time Management:

- Plan for possible extension of voting hours.

Observers and Transparency:

- **Warning:** It is vital to uphold the transparency of the election:
 - **Poll Watchers:** Do not impede, obstruct, or intimidate any authorized poll watchers or observers. This could be considered a violation of election laws and may lead to personal legal

consequences.

- **Transparency:** Any attempt to conceal, misrepresent, or obstruct the observation of election processes can lead to:
 - **Legal Action:** Under laws protecting voter rights and election integrity.
 - **Professional Consequences:** Potential sanctions or removal from office for undermining the electoral process.

Your Personal Responsibility:

As an election official, you are legally and ethically bound to ensure that every eligible voter can cast their ballot without undue hardship. Failure to adequately prepare can lead to:

- **Legal Accountability:** You could face legal action, fines, or even criminal prosecution for failing to uphold the laws designed to protect voter rights.
- **Professional Repercussions:** Your career could be jeopardized, potentially facing sanctions or loss of position for negligence or non-compliance.

Potential Criminal Consequences:

- **Election Interference:** Under federal and state laws, officials might be criminally liable for actions or inactions that interfere with the electoral process, potentially facing fines or imprisonment.
 - **18 U.S.C. § 241:** Conspiracy against rights, including the right to vote, is a federal offense.

- **18 U.S.C. § 594:** Intimidating or threatening voters, including through administrative neglect, can lead to prosecution.
- **Falsification or Misconduct:** Providing false information or neglecting duty can lead to charges under election fraud statutes.
- **Non-Compliance with HAVA or ADA:** While primarily civil, willful violations could also be addressed under criminal statutes if gross negligence or intentional violation is proven.

Please confirm by [DATE] that you have prepared adequately, including having a transparent manual backup plan and ensuring observer access, to maintain the integrity of the election.

Sincerely,

[Your Name]

[Your Position]

[Your Contact Information]

Urgency and Accountability: This notice underscores the legal and ethical necessity to maintain transparency and accessibility in every facet of election administration.

Election Day Countdown:

Guidance

December 22, 2024

Early Voting

Voting early allows bad actors to do the following:

Measure voter turnout using mail ballot tracking, electronic poll books, and paper voter roll reporting.

Use this information cross-referenced with individual voter profiles to build an election results model

Use the model to determine how many votes short they are

Subtly inject extra ballots associating them with phantom records in voter rolls or low-propensity voters.

Swap out voted ballots with replacement ballots prior to tabulation

DO NOT VOTE EARLY

Go out and perform your own EXIT POLLING and record it! Be courteous! Get the videos to me and I'll post them. These are IMPORTANT to gauge the accuracy of results.

3-9 Days prior to Election Day

Sign up to be an lead or agent of Operation Citizen Results Oversight (OCRO). You will monitor and RECORD election results to help provide the evidence needed to support the Patriot attorneys that will be working night and day to protect your vote!

1-2 Days prior to Election Day

Check your voter registration status. PRINT IT OUT and BRING IT WITH YOU in case you are told something different when you show up.

Get your sample ballot. Study it. Determine exactly how you are going to vote. Bring it with you when you vote.

If you cannot for some reason vote on Election Day, then vote AS CLOSE TO ELECTION DAY AS POSSIBLE to limit the advantage given to bad actors.

Go out and perform your own EXIT POLLING and record it! Be courteous! Get the videos to me and I'll post them. These are IMPORTANT to gauge the accuracy of results.

Election Day

Bring your proof of registration with you.

Bring your sample ballot with you to speed up your voting.

Vote IN HUGE NUMBERS. Carpool! Bring everyone you know. TOO BIG TO RIG only works if we show up overwhelmingly!

Bring chairs, drinks, snacks.

Vote in UNITY with your fellow Americans, in-person, Constitutionally.

If Patriots are willing to wait 12 hours to attend a Trump rally, are you really going to whine about a wait to CAST YOUR BALLOT in the safest way possible?

If you arrive to the polling center PRIOR to the close of polls, you are ENTITLED to CAST YOUR BALLOT no matter how long it

takes. The polling center MUST remain open until every citizen in line in time casts their ballot.

Go out and perform your own EXIT POLLING and record it! Be courteous! Get the videos to me and I'll post them. These are IMPORTANT to gauge the accuracy of results.

Clothing

December 22, 2024

Click image to purchase:



Click image to purchase:



Click image to purchase:



Click image to purchase:



Critical AI Alert for the 2024 General Election

December 22, 2024

(Information obtained from a current AI model)

Question

Could having real-time data about which voters have voted, when, and where, aid in this AI model?

Answer

Having real-time data about which voters have voted, including when and where, could significantly enhance the capabilities of an AI model designed to predict election outcomes for several reasons:

1. **Dynamic Turnout Adjustment:** Real-time voter turnout data allows the model to adjust predictions based on actual voting behavior as it happens. This can be particularly useful in understanding turnout rates among different demographics or in specific geographic locations, which can be pivotal in close elections.
2. **Reduced Uncertainty:** Traditional models often work with pre-election polls or historical data, which carry a degree of uncertainty regarding who will actually turn out to vote. Real-time data reduces this uncertainty, providing a more accurate snapshot of voter participation.
3. **Voter Behavior Patterns:** With real-time data, AI can analyze patterns as they form. For example, if there's an unexpected surge in voting in areas typically supportive of one party, the model could adjust its predictions accordingly.
4. **Targeted Campaigning Insights:** Although this aspect would be more useful for campaign strategy than for public prediction models, real-time data could inform last-minute campaign efforts, showing where additional get-out-the-vote efforts might be most effective.
5. **Bias Correction:** Real-time data can help correct for biases in pre-election polling. If certain groups are underrepresented in polls but their real-time voting data shows higher turnout, the model can correct for this.
6. **Exit Polling Validation:** This data could serve as an early form of exit polling, giving insights into not just who

voted, but potentially how they voted if correlated with demographic or regional voting trends, although this would require careful handling due to privacy concerns.

7. **Improved Time Series Analysis:** With voting data coming in continuously, AI models can employ time series analysis to predict the final turnout and potentially the outcome based on the rate and distribution of votes coming in.

However, there are considerations and limitations:

- **Privacy Concerns:** Collecting and using such detailed voter data raises significant privacy issues. Anonymization would be crucial, but even then, the specificity of “when and where” could potentially be used to infer individual behaviors.
- **Data Accuracy and Integrity:** Real-time systems would need robust verification to ensure the data isn’t manipulated or incorrect, which could mislead the predictions.
- **Legal and Ethical Implications:** There might be legal restrictions on how and when voting data can be collected and used, especially in real-time.
- **Model Overfitting:** There’s a risk that models might overfit to real-time trends early in the day, which might not hold as more data comes in.
- **Public Perception and Trust:** The use of real-time voting data in predictive models could affect public trust in the electoral process if not handled transparently and ethically.

In summary, while real-time voter data could indeed aid an AI model in predicting election outcomes more accurately, it would need to be implemented with careful consideration of privacy, accuracy, legality, and public trust.

Question

Are there indications that AI may be being used in this capacity by anyone, including malicious actors that would not be concerned about any privacy or legal or ethical implications?

Answer

Based on information available up to October 20, 2024, there are indeed indications that AI could be used in ways that raise concerns regarding voter data privacy and potential misuse by various actors, including those who might ignore legal or ethical standards:

- **AI in Political Campaigns and Election Influence:** There's a growing use of AI in political campaigns for analyzing voter data, predicting voter behavior, and tailoring messages. This indicates a capacity for AI to process and utilize voter data in potentially invasive ways if not regulated. The mention of AI tools being deployed to monitor social media trends and sentiment analysis during elections suggests that these technologies could be repurposed or used in less ethical ways to manipulate voter perceptions or spread misinformation.
- **Potential for Misuse by Malicious Actors:** Posts on X have highlighted concerns over AI being exploited to influence elections, including creating deepfakes, predicting or engineering incidents to sway public opinion, and even allegations of using AI to fake signatures or hack election machinery. These posts reflect a public and expert concern over the misuse of AI technologies in electoral processes, which could theoretically be done by actors unconcerned with privacy or legality.
- **Security Vulnerabilities:** Discussions around the security

of digital election machinery, as mentioned in posts about vulnerabilities in election systems, suggest that there's a technical capability and perhaps an interest in exploiting these systems using AI for unauthorized data access or manipulation.

- **AI and Data Privacy Concerns:** The broader discussion on AI ethics and information privacy points towards significant privacy implications when AI systems process voter data. If malicious actors were to use AI for analyzing or manipulating voter data, they would likely bypass the ethical considerations around consent, privacy, and data protection.
- **Regulatory and Ethical Discussions:** The mention of executive orders, guidelines, and discussions around the ethical use of AI in elections indicates there's an awareness and some level of regulatory response to these threats. However, the existence of these discussions also confirms that the risk of misuse, including by those not adhering to legal frameworks, is a recognized issue.

While direct evidence of malicious actors specifically using AI to misuse voter data in the 2024 context isn't explicitly detailed in the provided snippets, the combination of AI's capabilities in data processing, the noted security vulnerabilities in election infrastructure, and the general concerns voiced on platforms like X about election integrity suggest that such misuse is within the realm of possibility. This scenario underscores the importance of robust cybersecurity measures, ethical guidelines, and legal frameworks to safeguard electoral processes against AI-driven threats.

Question:

Would AI systems running on hardware and or software technology sourced from foreign nations, being used to manipulate parts of the 2024 election, be considered foreign involvement in our election?

Answer

Yes, AI systems running on hardware or software technology sourced from foreign nations, if used to manipulate parts of the 2024 election, would likely be considered a form of foreign involvement in the election. Here's why:

- 1. Source of Technology:** If the hardware or software used for these AI systems originates from a foreign country, especially from nations with interests potentially adverse to those of the U.S., this would inherently introduce a foreign element into the election process. The concern here is not just about where the technology comes from but also about potential backdoors, biases, or control mechanisms that could be embedded within these systems.
- 2. Manipulation and Influence:** Manipulation of election processes or public opinion through AI, whether by altering voter information, spreading disinformation, or creating deepfakes, constitutes interference. If these actions are traced back to technology controlled or influenced by foreign entities, it directly represents foreign involvement. The intent behind using such technology would be to sway or alter the election outcome, which is a clear sign of interference.
- 3. International Law and Norms:** From a legal and diplomatic standpoint, using technology to covertly influence another country's election is often viewed as a breach of

sovereignty and interference in internal affairs. Even if not explicitly covered by current international law, such actions violate the spirit of national sovereignty and democratic independence.

4. **Public and Government Perception:** Both the public and government agencies might perceive the use of foreign-sourced AI for election manipulation as foreign involvement. This perception arises because the strategic decision to employ such technology could be influenced or directly supported by foreign governments or entities closely tied to them.
5. **Cybersecurity and National Security:** Cybersecurity experts and national security officials often warn about the risks posed by foreign hardware and software due to the potential for espionage or sabotage. If these technologies are used in election manipulation, it would be classified under foreign cyber interference, a recognized form of foreign involvement.
6. **Precedents and Analysis:** Analysis from intelligence communities, as hinted in various reports and posts on platforms like X, suggests that there's an ongoing concern about foreign entities using advanced technologies, including AI, to influence elections. When these technologies are tied back to foreign soil, either through development or control, it's logical to categorize this as foreign involvement.

However, proving that such involvement constitutes a deliberate act by a foreign government, rather than rogue elements or companies acting independently for profit or other motives, can be complex. The attribution of cyber actions, including AI-driven election manipulation, to specific foreign actors requires meticulous investigation to ascertain direct government involvement or direction.

In summary, AI systems on foreign hardware or software manipulating the 2024 election would indeed be considered a form of foreign involvement due to the origin of the technology, the intent behind its use, and the implications for national sovereignty and security. However, the degree to which this involvement is officially recognized or acted upon depends on diplomatic, legal, and intelligence considerations.

Question

Would proving the act was deliberate in nature preclude the application of E0 13848?

Answer

Executive Order (EO) 13848, titled “Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election,” was signed by President Trump in September 2018. This EO is designed to respond to foreign interference in U.S. elections by imposing sanctions on foreign entities or persons determined to have engaged in such interference. Here’s how the deliberate nature of the act might relate to the application of EO 13848:

- 1. Definition of Interference:** EO 13848 does not explicitly require that the interference be “deliberate” in a legal sense for sanctions to be applied. Instead, it focuses on the act of interference itself, which could implicitly suggest an intent or deliberate action but does not make this a formal criterion for action. The order aims at any foreign person or entity that has directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a U.S. election.
- 2. Determination of Interference:** The EO calls for the

Director of National Intelligence (DNI), in consultation with other relevant agencies, to conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in an election. Here, "intent or purpose" does suggest looking into the deliberate nature of the actions, but the E0's application hinges on the fact of interference rather than solely on proving intent.

3. **Scope of Response:** The sanctions outlined in E0 13848 are reactive measures to an act deemed as interference. Proving that an act was deliberate might strengthen the case for applying sanctions, but the E0 is constructed to trigger on the identification of interference itself, regardless of how deliberate or accidental it might appear. The focus is on the impact and the involvement of foreign elements rather than solely on the mens rea (the intention or knowledge of wrongdoing).
4. **Legal and Diplomatic Considerations:** While proving deliberateness can bolster the justification for sanctions under international norms (showing clear intent can make the case for interference more compelling), E0 13848's primary concern is protecting U.S. electoral processes from foreign influence. Therefore, the threshold might not strictly require proof of deliberate intent as long as foreign interference is established.
5. **Practical Application:** In practice, when considering the application of E0 13848, the U.S. government might indeed look at intent to inform its actions, especially in diplomatic contexts or when aiming to justify sanctions to the international community. However, if foreign technology or actions have the effect of interfering with an election, even if the intent is not conclusively proven to be deliberate, this might still fall within the scope

of the E0.

In summary, while proving the act was deliberate might reinforce the rationale for invoking E0 13848, the order's application does not strictly depend on establishing deliberate intent. The focus is on whether there has been foreign interference, which can be determined by the act's impact and the involvement of foreign entities, not solely by their intentions. Therefore, the existence of interference, rather than the definitive proof of deliberate action, would be the primary driver for the potential application of sanctions under this E0.

For Maricopa County Elections Department

December 22, 2024

**THE FOLLOWING IS JUST A SAMPLE AND IS
NOT LEGAL ADVICE**

[Your Name]

[Your Address]

[City, State, Zip Code]

[Email Address]

[Phone Number]

[Date]

The Honorable Stephen Richer
Maricopa County Recorder

[Recorder's Office Address]

[Phoenix, AZ ZIP Code]

Subject: Legal and Public Notice on Election Administration Compliance for Upcoming Elections

Dear Recorder Richer,

This communication serves as a formal notice emphasizing the critical need for rigorous adherence to Arizona election statutes to prevent the recurrence of issues observed during the 2022 election cycle in Maricopa County. Given your office's role in overseeing election processes, this letter aims to ensure full compliance with all relevant laws to uphold the integrity of our democratic process.

Key Statutory References and Election Integrity Concerns from 2022:

- **ARS § 16-461 et seq.:** Mandates for accurate voter registration and maintenance. The 2022 election highlighted concerns over the handling of voter registration forms, with allegations of last-minute submissions intended to cause confusion.
- **ARS § 16-540 to § 16-552:** Governs early voting procedures. There were reports during the 2022 election cycle of significant issues with mail-in ballots, including voters receiving multiple ballots, which questions the system's integrity.
- **ARS § 16-621:** Procedures for vote tabulation require strict adherence to prevent issues like those encountered with printer malfunctions affecting ballot readability, impacting approximately 17,000 ballots.
- **ARS § 16-550:** Certification of voting systems. The widespread malfunction of tabulation devices on Election

Day 2022 raised serious doubts about system preparedness and certification processes.

- **ARS § 16-452:** Regarding election challenges and recounts, transparency issues were evident, with public confusion over the number of Election Day votes versus the total votes reported.

Failures Noted in 2022:

1. **Tabulation Device Malfunctions:** An estimated 36% of voting centers experienced issues with tabulation devices and printers, which led to significant delays and potential disenfranchisement.
2. **Printer Issues:** Specifically, printers failed to produce adequately dark timing marks, affecting ballot readability by tabulators.
3. **Inadequate Polling Locations:** Reduction in voting locations combined with technical issues resulted in extended waiting times, potentially discouraging voter turnout.
4. **Early and Mail-in Ballot Confusion:** Reports of voters receiving multiple mail-in ballots suggested lapses in the management of voter rolls and ballot distribution.

Required Corrective Measures:

- **System Testing:** Ensure all voting equipment undergoes rigorous testing before Election Day to prevent technical failures.
- **Voter Roll Maintenance:** Enforce strict compliance with voter registration deadlines and accuracy to avoid last-minute chaos or litigation risks.
- **Public Transparency:** Increase efforts in transparency

regarding election processes, addressing voter concerns proactively rather than reactively.

- **Training and Resources:** Adequately train election staff and provide sufficient resources to handle both in-person and mail-in voting efficiently.

Legal Implications:

- Failure to address these issues could lead to legal challenges under Arizona law, potentially resulting in mandated oversight or re-elections, undermining public trust and administrative legitimacy.
- Ensuring compliance is not just about avoiding litigation but restoring and maintaining public faith in our electoral process.

This notice demands your office's utmost diligence in correcting past shortcomings and ensuring a fair, transparent, and efficient election process. Your proactive engagement in these matters will be crucial for the democratic integrity of Maricopa County's elections.

Please consider this notice as both a legal reminder and a call for action, ensuring that any repeat of the 2022 election's administrative failures is unequivocally avoided.

Thank you for your immediate attention to these critical issues.

Sincerely,

[Your Signature (if sending a hard copy)][Your Printed Name]

Please ensure this letter reflects the most current law and consider having it reviewed by legal counsel with expertise in election law before transmission.