LETTER OF INTENT

Dear Secretary LaRose,

I am writing to formally inform you of my intent to pursue legal action should the forthcoming elections in Ohio fail to adhere to principles of fairness, transparency, and timely result reporting. Enclosed is a detailed report outlining the critical need for manual voting systems, the importance of election transparency, and the expectation for same-day election results.

I am compelled to address the critical issue of election security in Ohio, particularly in light of the FBI's warnings regarding cyber threats to electoral processes. This letter serves as both a notice of my intent to ensure election integrity and a formal request for transparency regarding the measures your office is taking to mitigate these threats.

Given the responsibilities outlined for various Ohio agencies in reducing the cyber threat surface:

Negligence in Ministerial Duties: Any indication of negligence in executing ministerial duties related to election security, particularly in threat reduction, will be considered a severe lapse in your office's obligations.

Demand for Plans and Cost Justifications: I demand to see detailed plans on how your office, in collaboration with the Ohio Department of Administrative Services, Ohio Homeland Security, and other relevant bodies, intends to safeguard our elections. Additionally, I request a transparent justification of costs associated with these security measures.

Transparency in Operations: There must be complete transparency in how these operations are conducted. Public trust in our electoral system hinges on knowing that every measure is taken to secure their vote.

Litigation Warning: Should the November elections face any issues attributable to cyber threats or lack of adequate preparation and transparency, I am prepared to initiate litigation. This action would aim to address any failures in ensuring a secure, fair, and transparent electoral process.

The citizens of Ohio deserve an election process free from both external threats and internal inefficiencies or negligence. Your office's cooperation in providing the requested information and ensuring robust election security will be pivotal in maintaining public confidence.

I look forward to your prompt response detailing the steps being taken to secure our elections, the allocation of resources for these efforts, and how you plan to keep the public informed throughout this process.

LETTER OF INTENT

This report has been compiled with the intent to:

- Highlight the cybersecurity benefits of transitioning to manual voting systems, reducing complexity and thus the risk of cyber threats as per the principles of parsimony in cybersecurity.
- Advocate for the responsible use of taxpayer funds by reallocating resources from vulnerable electronic systems to enhance broader critical infrastructure security.
- Ensure that election results are auditable, transparent, and available to the public on election day, thereby maintaining the integrity and public trust in our democratic processes.

Should the elections not meet these standards—specifically, if there is any indication of unfair practices, lack of transparency, or if the results are not made available on election day—I am prepared to initiate litigation to address these grievances.

This action is not taken lightly but is deemed necessary to uphold the democratic values upon which our state and nation stand. The citizens of Ohio deserve an electoral process that is beyond reproach, where every vote is counted accurately and reported promptly.

I trust that you will take the contents of the enclosed report into serious consideration and take all necessary steps to ensure our elections reflect the highest standards of integrity.

I look forward to your response and to seeing positive changes in our electoral process.

Sincerely,

Terpsehore Maras

Independent Candidate for Ohio Secretary of State

The Security of Our Electoral Processes: Reducing Cyber Threats Through Manual Ballot Counting

The security of electoral processes has become increasingly critical in the face of growing cyber threats that target electronic voting systems. The report highlights the necessity of adopting manual counting methods to enhance the integrity, transparency, and trustworthiness of the electoral process. This approach not only mitigates risks associated with cyber interference but also reallocates resources to strengthen overall infrastructure security, ensuring a resilient democratic framework.

Prepared by:
The Organization Regarding Everything -Think Tank
Terpsehore Maras (Cleveland, OH)

AUGUST 2024

The security of our electoral processes is critical, especially as cyber threats increase in sophistication. The principle of parsimony, or Occam's Razor, advocates for the simplest solution, which is often the most effective. Transitioning from electronic voting machines to manual ballot counting represents a straightforward and cost-effective strategy that significantly reduces cyber threat exposure.

A joint PSA from CISA and the FBI clarifies that while Distributed Denial of Service (DDoS) attacks might disrupt access to election information, they do not compromise the integrity of the voting process itself. However, this assurance only holds if the voting infrastructure remains isolated from such vulnerabilities. By removing electronic voting machines, we eliminate many potential cyber threats, including those beyond DDoS attacks, such as direct system breaches or ransomware that could affect electronic systems.

The joint PSA report emphasizes that even though DDoS attacks won't prevent voting or corrupt vote counting, the broader cybersecurity landscape suggests that any digital system can be a target for more severe forms of cyber interference. Adopting manual counting aligns with Occam's Razor by reducing complexity and avenues for cyber attacks. This shift simplifies the process and allows for the reallocation of funds from maintaining and securing complex electronic systems to other critical areas, enhancing overall election security and reinforcing public confidence in the electoral process. This approach isn't just about reducing threats but also about wisely managing resources, making it a prudent choice in safeguarding election integrity.

Enhancing Election Security through Parsimony and Resource Reallocation

This report proposes a pivotal transition to manual voting systems in an era of increasing cybersecurity threats. It champions the principle of parsimony in cybersecurity—where simplicity reduces risk—and advocates for judicious allocation of public funds. The recommendations aim to fortify the security, integrity, and public confidence in the electoral process. Moreover, this strategic shift promises to redirect resources toward protecting our most critical infrastructures from cyber vulnerabilities, ensuring the democratic process remains robust, transparent, and resilient against digital threats.

Parsimony in Cybersecurity: Reducing Complexity Reduces Risk

Simplicity Equals Security. Cybersecurity principles dictate that increased complexity correlates with more vulnerabilities exploitable by adversaries. The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) have identified electronic voting systems as targets for cyber threats, including DDoS attacks. These attacks could impair access to election-related information and erode public trust (CISA, 2024). Transitioning away from these systems reduces complexity and risk, significantly shrinking the cyber threat landscape.

: Cybersecurity principles dictate that increased complexity correlates with more vulnerabilities exploitable by adversaries. The FBI and the Cybersecurity and Infrastructure Security Agency have identified electronic voting systems as targets for cyber threats, including DDoS attacks, which could impair access to election-related information and erode public trust (Transitioning away from these systems reduces complexity and risk, significantly shrinking the cyber threat landscape.

Physical Evidence Over Digital Susceptibility. The shift to manually counted paper ballots offers a physical, verifiable voting record less vulnerable to cyber manipulation than digital alternatives. This approach simplifies the auditing process and upholds election integrity and transparency, aligning with security recommendations from election experts (CISA, 2024).

Negligence and Misuse of Taxpayer Dollars

Failure to Act as Negligence: Persisting with electronic voting systems, despite documented vulnerabilities, could be deemed negligent. Continuous advisories from CISA and the FBI underscore the cyber risks these systems face (CISA, 2024). Neglecting these warnings jeopardizes electoral integrity and betrays public trust in democratic processes.

Misallocation of Funds. Allocating public funds to maintain or upgrade known vulnerable systems represents a fiscal misstep. Research in the Journal of Cybersecurity advocates for secure, manual voting processes as a more cost-effective and safer alternative (CISA, 2024). Redirecting these funds towards fortifying other critical infrastructures, as identified by federal security agencies, represents a judicious use of taxpayer money**.**

Concrete and Foolproof Actions are Needed

DHS and FBI Recommendations: The Department of Homeland Security (DHS) and FBI have emphasized the necessity for robust measures to counter cyber risks in critical sectors, including electoral systems (CISA, 2024). The most straightforward and effective measure is the complete cessation of electronic voting machine use, eradicating the cyber threat at its source.

Scholarly Support for Manual Systems

Academic analyses endorse manual voting systems for their reduced susceptibility to cyber threats and capacity to produce auditable outcomes, crucial for electoral integrity (CISA, 2024). Not adopting these foolproof methods compromises election security and undermines the electorate's confidence in the democratic process.

Here are some sources and links from academic and governmental sources endorsing manual voting systems for their security benefits:

CISA's Election Security Resources

CISA provides tools and guidelines to enhance election cybersecurity, implicitly supporting methods that reduce cyber threats, like manual voting. For more information visit CISA's Election Security Page.

University of Michigan Study on EVMs in India

A study involving a University of Michigan computer scientist highlighted vulnerabilities in electronic voting machines (EVMs) used in India, suggesting manual systems could

be less prone to certain types of fraud. This was mentioned in a post by @tanmoyofc on X, referring to research publications or university statements for academic credibility.

The Atlantic Article

An article in The Atlantic titled "How Electronic Voting Could Undermine the Election" discusses computer security experts' skepticism towards electronic voting, indirectly supporting more traditional, manual methods for their simplicity and security. The article can be accessed via The Atlantic's archives or references in election security discussions.

Election Security Preparedness by EAC

The U.S. Election Assistance Commission (EAC) provides resources for election security. While not directly endorsing manual voting, the EAC emphasizes the importance of auditable outcomes, a feature inherent in manual voting systems. More can be found at www.eac.gov.

Posts on X

Various posts on X reflect ongoing discussions about election security. Some users, like @ESYudkowsky, mention the distrust among computer security researchers toward electronic voting machines, thereby indirectly supporting manual systems for their straightforward security benefits.

Feasibility and Speed of Transitioning to Manual Voting Systems

The transition to manual voting systems, which involves replacing electronic voting machines with hand-counted paper ballots, is both feasible and can be executed swiftly, but it depends on several critical factors:

Technical Implementation

Research suggests that operationally, transitioning to manual ballot counting could be completed relatively quickly. Some experts argue that a complete switch could be achieved within six months, given a clear plan and political will.

The technical aspect of printing and distributing paper ballots and organizing manual counting procedures is straightforward and doesn't require complex technological infrastructure.

Legislative and Policy Adjustments

Legal frameworks governing elections may need revision to accommodate a shift to manual systems. This could involve amending existing laws or passing new legislation, which can be time-consuming due to legislative cycles, debates, and the need for bipartisan support.

Changes in election laws typically require public consultations, committee reviews, and potential court challenges, which could extend the implementation timeline.

Public Education and Acceptance

Educating the public and training election workers on manual voting procedures are crucial for a smooth transition.

Historical evidence from countries like the Netherlands shows that comprehensive public education campaigns can help build trust in the manual system and ensure understanding of the processes involved.

Infrastructure and Logistics

Establishing or upgrading infrastructure for secure storage, transportation, and counting of paper ballots is significant.

This includes setting up secure facilities for ballot storage, ensuring safe transportation to counting centers, and organizing transparent and auditable counting processes.

These logistical considerations can impact the transition's speed and efficiency.

Practical Considerations and Phased Approach

While the physical transition to manual counting might be completed quickly, comprehensive implementation might require a phased approach.

Pilot programs in smaller jurisdictions could be used to test and refine manual counting procedures before scaling up to a statewide level.

Realistic Timeline and Variable Factors

While the physical transition to manual voting could be executed within months to a year, achieving full-scale implementation that ensures effectiveness, security, and public trust might take longer. The exact timeline would depend on several factors:

Urgency and Political Will

The transition could be expedited if prioritized and backed by strong political support. Historical precedents show that rapid policy shifts can occur under significant public and political pressure, as seen in Germany's swift adaptation of voting procedures post-WWII.

Resource Allocation

Adequate funding and resource allocation can accelerate the process. Ensuring sufficient training, public awareness campaigns, and logistical support are crucial for a smooth transition.

Political Landscape

Political dynamics, including partisan perspectives on election security, can influence the speed and scope of implementation. Achieving bipartisan consensus is often necessary for comprehensive electoral reforms.

While a transition to manual voting systems can be operationally quick, comprehensive implementation, including necessary legal changes, public education, and logistical infrastructure, might realistically take a few years. This timeline ensures the transition is conducted effectively, securely, and with public trust. Considering these factors, Ohio and other states could achieve a secure, transparent, and trusted election system, aligning with best practices observed in other democracies and recommendations from cybersecurity experts.

References

- CISA and FBI Release Joint PSA on Potential Election DDoS Attacks
- Verified Voting on Election Security
- Election Lab on Manual Counting Practices (REMOVED in 2020 -links dead)
- National Democratic Institute on Election Security (REMOVED in 2020-links dead)

In the United States, each state has various agencies with ministerial duties to reduce the threat surface in elections and beyond. Ministerial duties are obligations where public officers have little to no discretion; they must perform these duties as mandated by law, with actions directed by clear and positive commands. These duties are crucial in the context of election security, where the integrity and safety of the electoral process are paramount.

OHIO AS A REFERENCE

Ministerial Duties and Legal Responsibilities for Reducing the Threat Surface in Ohio

In Ohio, several key state agencies are responsible for reducing the cyber threat surface, especially concerning election security. These agencies must implement adequate cybersecurity measures, uphold public trust, and maintain the integrity of Ohio's critical infrastructure, including its electoral systems. This duty is legally required by state and federal law, emphasizing the essential role of transparency, accountability, and proactive security management.

Ohio Secretary of State’s Office

As the chief elections officer, the Ohio Secretary of State is primarily responsible for overseeing election administration and implementing cybersecurity measures to protect election infrastructure. Under Ohio Revised Code (ORC) § 3501.05, the Secretary of State is charged with "preparing rules and instructions for the conduct of elections," ensuring that voting systems are secure and protected against cyber threats. This office collaborates with federal entities such as the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) to incorporate best practices and threat intelligence into Ohio's election security strategies. Failure to act on these responsibilities or implement adequate cybersecurity measures could expose the Secretary of State's office to accusations of negligence and breach of ministerial duties.

Ohio Department of Administrative Services (DAS)

The DAS, mainly through its Office of Information Technology (OIT), is crucial in managing and securing the state's IT infrastructure, including election-related systems. According to Ohio Revised Code § 125.18, the DAS is responsible for "protecting the state's computer systems and telecommunication networks." This mandate includes providing cybersecurity guidance, tools, and support to secure systems critical for elections. DAS must ensure that all state-run information systems, including those used in elections, adhere to stringent cybersecurity protocols to mitigate risks and vulnerabilities.

Ohio Department of Public Safety (DPS) – Ohio Homeland Security

Under Ohio law (ORC § 5502.01), the Department of Public Safety, through its division of Ohio Homeland Security, is tasked with protecting the state from various threats, including cyberattacks. This agency coordinates with state, federal, and local partners to monitor, detect, and respond to cyber threats. Ohio Homeland Security's role includes conducting vulnerability assessments and ensuring that cybersecurity strategies are integrated into the broader public safety framework. This holistic approach to security underscores the agency's obligation to protect both election infrastructure and other critical sectors.

County Boards of Elections

At the local level, County Boards of Elections are entrusted with administering elections in compliance with state guidelines set forth by the Ohio Secretary of State. These boards are responsible for implementing specific security measures tailored to local needs and ensuring that all staff are adequately trained to recognize and respond to cyber incidents. According to Ohio Revised Code § 3501.11, these boards must "conduct all elections held in the county" and "ensure the security of voting equipment and the accuracy of vote counting," highlighting their critical role in maintaining election integrity and public trust.

Ohio National Guard Cyber Protection Team

The Ohio National Guard, through its Cyber Protection Team, may be called upon to provide specialized cybersecurity assistance in response to significant threats to the state's infrastructure, including election systems. This team offers additional resources and expertise, helping to bolster Ohio's defenses against cyber threats. Their involvement highlights the need for a coordinated state and federal response to complex cybersecurity challenges.

The ministerial duties of these agencies underscore a collective responsibility to reduce the surface of cyber threats and ensure the security of Ohio's elections. By law, these agencies must operate with transparency, accountability, and a commitment to public trust. Failure to adequately explain new procedures, justify expenditures, or address vulnerabilities risks public confidence and exposes these agencies to legal liability for negligence and misuse of public funds. Clear, proactive communication and transparent security measures are essential to fulfill their statutory and ethical obligations, protect the electoral process, and maintain the integrity of Ohio's democracy.

Nationwide, state agencies, from Departments of State to local law enforcement, execute these duties to safeguard against threats ranging from cyberattacks on voting infrastructure to physical threats against election officials. This framework ensures the democratic process remains secure, transparent, and resilient against internal and external threats, thereby maintaining public trust in election outcomes. As stated by law, they have a **DUTY** to **REDUCE THREAT SURFACES** and **JUSTIFY** costly methods and methods that hinder transparency through information classification - such actions put concrete boots on democracy.

CYBER THREAT SURFACE REDUCTION

Reinforcing critical infrastructure like electrical grids, water systems, and other utilities with funds redirected from the maintenance of electronic voting machines represents a strategic reallocation of resources toward broader security benefits. Here's how this approach can be justified:

Reduced Cyber Threat Surface

By transitioning from electronic voting machines to paper ballots, the cyber threat surface associated with elections is virtually eliminated. This move reduces the need for continuous cybersecurity measures specific to voting technology, freeing up funds.

Infrastructure Resilience:

Electrical Systems: The electric grid is vulnerable to cyber-attacks, which could lead to widespread power outages. Funds could be used for:

- Upgrading outdated infrastructure to more secure, modern systems.
- Implementing advanced cybersecurity measures, such as intrusion detection systems, better encryption, and secure off-site backups for grid management systems.
- Developing intelligent grid technologies that can autonomously respond to detected anomalies or attacks.

Water Systems: Water supply systems face threats from both cyber and physical attacks, which could lead to contamination or service disruption. The investment could go towards:

- Securing SCADA (Supervisory Control and Data Acquisition) systems that manage water treatment and distribution.
- Physical security enhancements at water facilities.
- Redundancy systems to ensure continuous operation in case of an attack or failure.

Comprehensive Security Approach

Instead of focusing security efforts on one sector (elections), the funds can bolster a multi-sector defense strategy. This holistic approach improves the resilience of multiple infrastructures against not just cyber threats but also natural disasters and physical attacks.

Public Trust and Safety

While public trust in elections is crucial, ensuring the safety and reliability of daily necessities like electricity and water might have a more immediate impact on public confidence and safety. This shift can demonstrate a government's commitment to protecting essential services.

Cost Efficiency and Long-term Savings

Electronic voting machines require updates, maintenance, and eventual replacement. Paper systems, while having their costs, generally incur fewer ongoing cybersecurity expenses. The saved funds can be invested in infrastructure that benefits from technological advancements, potentially leading to long-term operational savings.

Education and Workforce Development

Some funds could also be directed towards education programs for cybersecurity, engineering, and infrastructure management, thereby creating a more skilled workforce to manage and protect these critical systems.

Community and Economic Stability

Reliable infrastructure supports economic activity by ensuring businesses can operate without interruption. This stability can attract investment and foster economic growth, indirectly generating more resources for further infrastructure improvements.

The case for redirecting funds from the upkeep of electronic voting machines to the fortification of general infrastructure underlines a strategy to boost society's resilience against various threats. This strategy recognizes that while electoral integrity is crucial, it can be effectively secured through hand-counted paper ballots. This shift not only simplifies election security but also liberates substantial financial resources. These resources can then be invested in strengthening the essential infrastructure that underpins a state or nation's health, safety, and economic stability.

This strategic reorientation from niche security protocols to a holistic protective framework fundamentally underscores the critical role of transparency in forging cost-effective and efficacious solutions. Transparency is not merely a procedural enhancement but a cornerstone ensuring security measures' integrity and efficiency, particularly in safeguarding the populace's daily necessities and economic stability.

TRANSPARENCY IS KEY

> If.Corruption.is.a.disease?transparency.is.a.central.part.of.its.treatment¡.ΩKofi.Annan

Transparency should be a central mechanism for all government actions, including state and federal operations and services. This principle applies equally to cybersecurity and election integrity. Transparency in operations, especially in systems as pivotal as election infrastructure, ensures that every process is accountable, reducing the risk of hidden vulnerabilities and enhancing public trust.

Furthermore, Cost-Effectiveness through Openness is ideal. Many studies on this notion exist. The one by Sheppard and Beck (2023) on the transparency trade-offs in national Public-Private Partnership units illustrates how open governance practices can lead to more economically viable solutions by preventing mismanagement and corruption. This approach can be directly correlated to the management of election technologies, where transparency in procurement, maintenance, and operation of voting machines could drastically cut unnecessary costs and redirect funds towards more pressing security enhancements.

Efficacy, not Efficiency, is imperative in Election Security: Transparency in election systems enhances public trust and financial accountability and points towards a broader consensus: transparent systems are inherently more secure because they allow for public scrutiny, audibility, and verification. As the FBI and DHS warned, this is crucial for elections where electronic voting machines have been criticized for opacity, potentially harboring vulnerabilities.

Finally, by eliminating the opaque nature of electronic voting systems in favor of transparent, manual counting processes, we not only heed the warnings of cybersecurity threats but also embrace a model where cost-effectiveness and solution efficacy are maximized through transparency. This shift not only defends against cyber threats but does so in a manner that is open, verifiable, and, thus, inherently more secure and trusted by the public. This isn't just a theoretical proposition but is backed by the need for transparent, accountable systems in all sectors, particularly those as critical as national elections.